Republic of Panama
Superintendency of Banks

RULE N°. 1-2019
(dated 19 March 2019)

"Red Flags Catalog for Detecting Operations related to the Financing of Terrorism"

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 paragraphs 1 and 2 of Article 5 of the Banking Law, safeguarding the soundness and efficiency of the banking system and strengthening and fostering favorable conditions for the development of the Republic of Panama as an international financial center are objectives of the Superintendency of Banks;

According to Paragraph 5 of Article 11 of the Banking Law, the Board of Directors is responsible for establishing the administrative interpretation and scope of the legal and regulatory provisions on banking matters;

Article 112 of the Banking Law provides that banks and other entities supervised by the Superintendency will be required to establish policies, procedures and 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;

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

Article 19 of Law 23 of 2015 establishes the Superintendency of Banks, among others, 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 of legal entities and other legal arrangements, is among the duties of the supervisory bodies;

Pursuant to the provisions of Article 22 of Law 23 of 2015, amended by Article 123 of Law 21 of 2017, the Superintendency of Banks is responsible for supervising the financial reporting entities on the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction;

For the purposes of Article 54 of Law 23 of 2015, the financial reporting entities must communicate directly with the Financial Analysis Unit (UAF, for its acronym in Spanish) on any event, transaction or operation which they suspect may be related to the crimes of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, regardless of the amount and whether or not it can be confirmed or supported;

By means of Administrative Resolution 33-2018 dated 25 September 2018, the Financial Analysis Unit provided the adoption of Guidelines and Compendia in matters of the financing of terrorism as a useful tool for Supervisors and Reporting Entities in order to fight the financing of Terrorism;

FATF's 40 Recommendations are a coherent international standard that countries must effectively put in place through legal, regulatory and operational measures in order to have a sound domestic

system that enables combating money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction;

[One of] the Financial Action Task Force's (FATF) Recommendations establishes that whenever a financial institution suspects or has reasonable grounds to suspect that the funds are proceeds of criminal activities or are related to the financing of terrorism, the financial institution must be required by Law to immediately report its suspicions to the Financial Intelligence Unit, which in our case is the Financial Analysis Unit (UAF);

During its working sessions, the Board of Directors determined it was necessary and advisable to establish, by means of a Rule, a Red Flags Catalog for detecting operations related to the financing of terrorism, based on the Compendia of relevant risk indicators for the detection of the Financing of terrorism issued by the Financial Analysis Unit.

RESOLVES:

ARTICLE 1. SCOPE. The provisions herein will be applicable to the following reporting entities:

a. Banks and/or banking groups;
b. Trust companies;
c. Finance companies;
d. Leasing companies;
e. Factoring companies;
f. Issuers or processors of debit, credit and prepaid cards, whether individuals or legal entities, including those issuing and operating their own cards;
g. Issuers of payment instruments and e-money;
h. Banco de Desarrollo Agropecuario (Agriculture Development Bank);
i. Banco Hipotecario Nacional (National Mortgage Bank);
j. Home savings and loans companies;
k. Other trust corporate services providers.

Only the red flags related to the activities conducted by the reporting entities listed in items c, d, e, f, g, j, and k will be applicable to them.

ARTICLE 2. RED FLAGS CATALOG. The red flags catalog below must be adopted. This catalog includes customer or corporate behavior, as well as the characteristics of certain financial operations that may lead to the detection of a suspicious operation related to the financing of terrorism, which may not necessarily be listed herein.

Reporting entities must examine the operations and/or behaviors indicated herein with special attention, in order to determine, taking into consideration other flags, factors and criteria, whether they are suspicious operations related to terrorism financing risks.

ARTICLE 3. RED FLAGS RELATED TO CUSTOMER BEHAVIOR. Reporting entities must pay special attention to the following behaviors or actions adopted by customers:

1. A customer with mobile telephone numbers that are known or suspected to be used by terrorists or [persons] suspected [of committing terrorist acts];

2. A customer that is suspected of being a supporter, sympathizer or clandestine facilitator of violent extremism or radicalization or that is involved with or related to terrorists, terrorist groups or organizations of this nature;

3. A customer that rejects the cultural standards of the country where he is conducting the operation and makes great efforts to avoid personal contact with some bank employees (e.g. refuses to interact with female employees;

4. A customer with a behavior indicating the he is adhering to radical or extremist ideas or presenting violent trends (e.g. social media profiles showing multiple postings of articles related to or about sympathizers of terrorist organizations);

5. New customers asking excessive questions of bank employees on disclosures, reporting, thresholds or recordkeeping requirements;

6. Accounts opened on behalf of a legal entity that has the same address as another individual that is not associated with the account;

7. A customer opening several accounts (e.g. bank accounts, prepaid cards, e-wallets, etc.) for receiving and/or sending low denomination wire transfers;

8. A customer opening an account for the sole purpose of receiving one or more wire transfers and withdrawing or transferring money to third parties;

9. Opening accounts in regions other than those were the customer lives or resides and with no reasonable purpose.

ARTICLE 4. RED FLAGS RELATED TO THE CUSTOMER ECONOMIC PROFILE. Reporting entities must pay special attention to the following patterns or circumstances related to the customer economic profile:

1. Individual accounts receiving multiple large value wire transfers from people not related to them or from unknown sources (e.g. the declared purpose is “food”);

2. A customer presenting different identification documents every time the entity requests one;

3. A customer that, during the course of business, uses aliases, nicknames, or other alternative or simplified expressions instead of his (full) name. This could include name transposition;

4. Wire transfers requested by different persons or entities sharing one or more personal details (e.g. name, address, employer, telephone number, etc.) on the same or contiguous dates;

5. The frequency or volume of operation is inconsistent with the occupation, the income or the age of the customer;

6. A sudden, significant withdrawal (generally in cash) of benefits earned over a period of months.

ARTICLE 5. RED FLAGS RELATED TO GEOGRAPHIC FACTORS. Reporting entities must pay special attention to the customer transactions or operations related to the following geographic factors:

1. The originator of an operation and the beneficiary of funds that could be related to a high-risk jurisdiction or region;

2. A customer whose nationality, residence or place of business is located in high-risk jurisdictions or regions;

3. Customers making wire transfers to persons in areas of conflict, i.e. those high-risk jurisdictions/regions that are unstable, that are at war, where armed hostility is present or where terrorist organizations are active;

4. Customers making wire transfers to people in provinces/regions with known links with terrorist organizations or that share borders with territories controlled by terrorist organizations;

5. Customers making wire transfers to jurisdictions/regions that are transit zones or that have had a flow of money to/from known foreign terrorists;

6. Customers making wire transfers to jurisdictions with strategic deficiencies in the system for the prevention of money laundering and the financing of terrorism, weak institutional frameworks or those that do not comply with Financial Action Task Force standards;

7. Customers making wire transfers to countries where funds and other assets are generated for terrorist acts or terrorist organizations, regardless of where these acts are conducted or where the organizations reside;

8. Various persons sending funds to the same beneficiary in a high-risk jurisdiction;

9. The same customer sending funds to many beneficiaries in a high-risk jurisdiction;

10. High frequency cross-border transfers of securities to/from persons not connected or related;

11. Sending/receiving funds to/from the same counterparties of persons that seem to act separately. (i.e. also known as a “consumers network,” which represents a number of persons connected by common counterparties);

12. A payment from abroad with a description of the operation such as donation, help, loan, etc., and its immediate cash withdrawal or immediate wire transfer to another account;

13. Excessive funds paid to an account held by a student in a foreign country by a family member or an unrelated organization;

14. Customers residing in a high-risk jurisdiction or related to it;

15. Customers accessing bank facilities through the Internet (online) from an IP address located in an area of conflict or an address not related to the customer due diligence records;

16. A customer shows significant expenses abroad in an account opened recently;

17. An indication that the customer has travelled (or travels regularly) with cash to areas in or near areas of conflict.

ARTICLE 6. TRANSACTIONS RELATED TO KIDNAPPING FOR RANSOM. Reporting entities must pay special attention to transactions that could be related to kidnapping for ransom, a source of income for terrorist groups. Some indicators identified and involved in kidnapping for ransom are listed below:

1. Relatives (on behalf of the victim) that acquire money from the sale of assets or loans;

2. The establishment of a trust fund (or another legal arrangement) to collect/store donations for ransoms;

3. The establishment of a *crowdfunding* website to accept donations on behalf of the victim;

4. International wire transfers under the name of religious groups or entities. People (e.g. treasurers) controlling bank accounts on behalf of religious organizations that, when the banks ask them, indicate that the true purpose of the operations was, in fact, to pay ransoms;

5. Cash withdrawal from accounts concealed for use as aid payments;

6. Funds received from an insurance company marketing kidnapping and ransom insurance products.

ARTICLE 7. RED FLAGS RELATED TO EXPENDITURE. Reporting entities must pay special attention to the following behaviors related to customer expenditure:

1. <u>Expenditures related to trips</u>:

    a. Payments in outdoor activity shops (where they can get boots, sleeping bags, clothing, thermal underwear, tents and equipment)

b. Payments indicating medical appointments before travelling;

c. Purchase of airplane tickets, bus tickets, car rentals, transportation booking services;

d. One-way airfare bookings with a credit card (generally for people without an definable direct relationship);

e. Purchase of numerous airplane or bus tickets, after receiving various wire or cash transfers;

f. Payment of visas, particularly online bank payments for electronic visas to areas of conflict;

g. Travelers asking questions to confirm that the nominated beneficiaries of life insurance policies would receive the payment in circumstances that may arise from participating in terrorism and not from being the victim of terrorism. (These cases involve potential foreign terrorist fighters not declaring their trips to areas of conflict before their departure);

h. Young people purchasing funeral or life insurance policies or collecting a policy for paying airplane tickets.

i. Purchase of cars to be exported to countries bordering areas of conflict.

2. Expenditure unrelated to trips:

a. Purchase of expensive and sophisticated communication and information technology devices (e.g. satellite telephones);

b. Purchase of shooting games or attending combat-related training activities;

c. Purchase of weapons or dual use products that could be used for terrorist attacks or in a war context (e.g. ammunition, explosive material, military supplies, electronic or optical equipment) through e-payment accounts;

d. Payment to media or libraries related to propaganda on radicalism, extremism or violence;

e. Donation to nonprofit organizations or religious websites related to propaganda on radicalism, extremism or violence;

f. Purchase of many prepaid cards (e.g. telephone, general purposes).

ARTICLE 8. RED FLAGS RELATED TO PRODUCTS OR SERVICES. Reporting entities must pay special attention to the following transactions related to products and services:

1. Risk indicators for identifying suspicious suppliers:

a. Extensive use of collection accounts (where small amounts of money are deposited or added and then transferred overseas in periodic intervals);

b. Wire transfers frequently sent by businessmen to foreign countries that have no commercial connection with the host countries;

c. Commercial accounts used to send or pay large amounts of money but that almost never show regular activities related to the business, such as payment of wages, invoices, etc.;

d. Frequent deposits of third party checks and money orders to commercial or personal accounts.

2. General indicators involving cash and ATMs:

a. Sudden withdrawal of money, approximately the current balance of the account, justified as a need to travel abroad;

b. The customer requests the withdrawal of funds in cash previously transferred to his personal account in a short period of time after the first operation;

c. The customer requests the payment in cash of the unused balance of his account;

d. The structuring of cash deposits in smaller operations to avoid reporting requirements above the specific threshold;

e. Various withdrawals from a single ATM on consecutive days or making various withdrawals from different ATMs in nearby locations;

f. Cash withdrawals using debit cards on the same day or consecutive days, in different countries throughout an identifiable route to an area of conflict;

g. Small amounts of cash frequently deposited in self-service terminals to private accounts (the account is used to collect donations) and the withdrawal of the funds collected through self-service terminals shortly afterwards;

h. Large amounts of money deposited, followed by low-denomination wire transfers under the reporting threshold;

i. Structured deposits in a third party account, followed by immediate withdrawals in an ATM abroad in transit areas or high-risk jurisdictions;

j. Individual accounts that suddenly switch [their] typical activities, such as numerous deposits conducted through ATMs and then repetitive balance consultations through phone calls, followed by the withdrawal of large amounts of money through ATMs.

3. <u>Specific indicators identified for credit cards:</u>

a. Repetitive cash advances in many countries near areas of conflict or countries that are on the route usually followed to/from areas of conflict;

b. Credit card payments in various countries during transit (e.g. gas stations, highway tolls or locations near an airport);

c. The customer shows high denomination cash advances in a recently issued credit card;

d. Cash advances in credit cards generally without immediate payment;

e. Given the customer’s credit capacity, an unfounded or unjustified request for a maximum increase in the credit limit;

f. Reaching credit limits before departing on a trip;

g. Sudden use of credit cards in high-risk territories (e.g. increased cash withdrawals) when the use was preceded/followed by a few inactive months;

h. Use of credit cards registered to third parties.

4. <u>Indicators identified for bank/personal loans:</u>

a. Customers applying for cash bank loans and tending to miss payments;

b. The customer’s use of bank loan funds not consistent with the declared purposes;

c. A customer applying for a high personal loan and shortly afterwards withdrawing a significant amount in cash;

d. Taking small loans with various loan/credit corporations and not paying them;

e. Loans granted (e.g. based on false income tax declarations) when there are indications that the persons can flee abroad;

f. Taking out frequent loans using high-value items as collateral;

g. Loan applications that seem unjustified given the applicant's economic and financial background;

h. Fraudulent loan applications to purchase goods that seem not to have been used by the applicants (e.g. purchase of vehicles or electronic devices).

5. Risk indicators for products and services of new payments:

a. Online payments:

a.1. A person using multiple financial profiles (e.g. e-wallets) to register in multiple payment systems;

a.2. An e-wallet registration from a high-risk jurisdiction/area;

a.3. Replenishment of the account from a high-risk jurisdiction/area;

a.4. Remote wire transfer of cash from an e-wallet to third party accounts opened in a different jurisdiction (person-to-person);

a.5. Payments indicating that the account may be used to collect funds for charities;

a.6. Multiple bank accounts from banks located in various cities used to fund the same account;

a.7. Online accounts linked to persons related to terrorism charges by name, credit card, addresses, e-mail activity and computer cookies (e.g. these accounts were used to buy electronic devices and prepaid mobile phone cards online);

b. Specific indicators relevant to prepaid cards:

b.1. Foreign prepaid cards issued in high-risk jurisdictions;

b.2. Use of prepaid cards registered under false identities or under another person's name for online purchases;

b.3. Cards charged through anonymous payment instruments (e.g. coupons paid in cash, cash amounts through ATMs, e-wallet);

b.4. Multiple purchases of prepaid cards that do not require identification, despite the fact that the rates are higher than those of a prepaid card with a higher threshold but requiring identification;

b.5. Purchase of multiple prepaid cards in exchange bureaus during currency exchanges;

b.6. Numerous cash deposits in a rechargeable prepaid debit card by subjects identified as having connections to terrorism.

ARTICLE 9. RED FLAGS RELATED TO NONPROFIT ORGANIZATIONS. Reporting entities must pay special attention to the following transactions related to nonprofit organizations:

1. Donations:

   a. Large cumulative amounts and amounts not properly justified, especially if they were made mainly in cash;

   b. Multiple cash deposits to a personal account (or with a condition that establishes that the cash must be transferred to an individual from a high-risk country) described as “donations” or “contributions for humanitarian help” or similar terms;

   c. High percentage of donations/assets in a nonprofit organization coming from or going to foreign states that do not belong to the donor’s financial location;

   d. Large amounts of donations coming from a fictitious individual to a nonprofit organization;

   e. Deposits using a combination of atypical monetary instruments to a legitimate commercial activity;

   f. Nonprofit organizations with operations in areas of conflict receiving donations from corporations (with commercial interests in these areas) in their accounts directly or through a series of structured operations. These funds may be related to terrorist organizations that extort these corporations through nonprofit organizations;

2. Expenditures:

   a. Organizations that have no intention to provide humanitarian help, sending money to high-risk jurisdictions;

   b. Operations expressing the purpose of building a facility for a nonprofit organization, especially if the beneficiary is an individual that does not seem to be connected with the project and that does not appear to be in the construction business;

   c. Use of charity organizations to sell merchandise;

   d. Merchandise paid by a third party, not the importer;

   e. The expenditures of the nonprofit organization on paper are not consistent with its expectations (e.g. the risk of the funds being embezzled, being given another purpose, or are subject to taxes with the objective of financing terrorism).

3. Operations:

   a. Transferring most of the collected funds to geographic areas usually affected by activities or initiatives related to the financing of terrorism;

   b. Requested operations with counterparties that appear on lists [of persons or entities related to the financing of terrorism] or that are related to the financing of terrorism activities.

4. Senior executives and other staff of nonprofit organizations:

   a. Incomplete data on the issuer of operations for the benefit of a nonprofit organization or for the benefit of individuals related to the organization;

   b. Directors (or employees) of a nonprofit organization who misappropriate funds, e.g. when the funds are withdrawn before departing from an area of conflict;

   c. The bank accounts of senior executives or contractors who have operations in areas of conflict may be paying terrorist organizations for extortion/ransom, looking out for their commercial interests or collecting extortions for them.

ARTICLE 10. RED FLAGS RELATED TO TRADE AND COMMERCIAL ENTITIES. Reporting entities must pay special attention to the following trade activities conducted by their customers:

1. Individuals involved in trading and producing goods and technology subject to designation or to specific financial sanctions nationally or globally;

2. Trade relationship established by individuals or legal entities that may be connected to a terrorist organization;

3. A large number of persons authorized to conduct operations on behalf of a legal entity or organization;

4. Wire transfers of money to high-risk jurisdictions immediately after the establishment of a legal entity, when a trade relationship has not been established yet;

5. Trade activities using cash through money or securities transfer services for operations instead of electronic wire transfers;

6. Operational activity among individuals or entities with corporations recently established without an apparent commercial relationship or corporations that apparently have no operations (e.g. import/export generic activity, without website, etc.);

7. Many incoming personal checks deposited in trade accounts without apparent legitimate purpose;

8. Travel agencies facilitating religious pilgrimages to destinations in high-risk jurisdictions and with an offered average cost significantly lower than the price of other travel agencies;

9. The legal entity's registered business line does not match its real trade activity, or the real beneficiary of the goods ordered does not appear to be the final beneficiary;

10. Numerous incoming wire transfers to commercial accounts without an apparent legitimate purpose;

11. Trade entities with businesses in high-risk areas having operations with goods that could be considered dual use or that could be used in terrorist activities;

12. Trade entities engaging in commercial activities in high-risk areas that could be vulnerable to abuse or coercion (e.g. payments in exchange of access to ports and trade activities controlled by terrorist groups);

13. Investment of funds in the establishment/operation of corporations purchasing/selling vehicles in high-risk areas of conflict.

ARTICLE 11. RED FLAGS RELATED TO THE ILLEGAL TRADE OF ANTIQUITIES/CULTURAL HERITAGE. Reporting entities must pay special attention to the following operations conducted by their customers:

1. Financial operations related to cultural property similar to those mentioned in United Nations Security Council Resolution 2199 and by the International Council of Museums (ICOM) in the Emergency Red List of Syrian Antiquities at Risk (2003), Emergency Red List of Syrian cultural Objects at Risk (2013) and the Emergency Red List of Libyan Cultural Objects at Risk (2015);

2. Financial operations related to antiquities coming from Iraq and Syria (including small pieces, such as coins and statuettes) on sale through the Internet and social media;

3. Financial operations related to sending subterranean control/scanning equipment, such as metal detectors used by looters to dig antique artifacts and cultural objects;

4. False import declarations indicating that the artifacts are coming from countries bordering Syria and Iraq.

ARTICLE 12. RED FLAGS RELATED TO THE PETROLEUM AND GAS INDUSTRY. Reporting entities must pay special attention to the following transactions related to the fuel and gas industry conducted by their customers:

1. Financial connections with corporations, agents and suppliers of spare parts [for the petroleum industry] located in high-risk areas;

2. Individuals or entities that suddenly buy and/or send petroleum equipment to Syria, Iraq or border states, when the activity is not consistent with the customer's business line;

3. Shell companies used to simulate trade and sale of petroleum products and spare parts related to [the petroleum industry];

4. An operation involving potential shell companies (e.g. companies that do not have a high capitalization level or show other indications of being a shell company);

5. A freight company is consigned as the final destination of the product;

6. Wire transfer or payment instructions from or due to parties not identified in the original letter of credit or other documentation;

7. A new customer requests an operation with a letter of credit that is pending the approval of a new account;

8. The operation involves the use of letter of credits suddenly amended or frequently postponed.

ARTICLE 13. ENACTMENT. This Rule will become effective upon its promulgation.

Given in the city of Panama on the nineteenth (19th) day of March, two thousand and nineteen (2019).

FOR COMMUNICATION PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN, **THE SECRETARY,**

Luis Alberto La Rocca Joseph Fidanque III