The Official Gazette

(EXTRAORDINARY)

OF GUYANA

Published by the Authority of the Government

GEORGETOWN, SATURDAY 2ND SEPTEMBER, 2023

TABLE OF CONTENTS **PAGE**

Bank of Guyana... 2760

FIRST SUPPLEMENT

LEGAL SUPPLEMENT

A. ACTS — NIL

B. SUBSIDIARY LEGISLATION — NIL

C. BILLS —NIL

GEORGETOWN, Demerara – Printed and Published every Saturday and on such Extraordinary Days as may be directed by the Government by Guyana National Printers Limited, 1 Public Road, La Penitence, Greater Georgetown.

SATURDAY 2ND SEPTEMBER, 2023

BANK OF GUYANA

AMENDMENTS TO SUPERVISION GUIDELINE (SG) NO. 13

SG No. 13 is now amended to include the following:

1. Part 2 section 2.2 - Supervision and Regulation of Financial Groups:
   - Risk Based Approach
   - Foreign Branches and Subsidiaries

2. Part 2 section 2.3 - Other Forms of International Cooperation
   - Safeguards on Information Exchanged

3. Part 2 section 2.5 - Tipping Off

4. Part 5 section 5.1 - Customer Due Diligence (CDD)
   - Reliance on Third Parties
   - CDD for Beneficiaries of Life Insurance Policies

5. Part 5 section 5.3.8 - Politically Exposed Persons

6. Part 5
   - section 5.4.3.2 - Cross- Border Wire Transfers
   - section 5.4.3.3 - Domestic Wire Transfer

7. Part 9 - Proliferation Financing

2.2. Regulatory Framework

The primary responsibilities of the BOG as a Supervisory Authority include:-

(a) reviewing the AML/CFT compliance programme of all financial institutions to determine its adequacy and assess its compliance with applicable laws and Guidelines and AML/CFT measures consistent with FATF Recommendations to the extent that host countries laws and Regulations permit;

(b) issuing Guidelines,[9] circulars or recommendations as appropriate to aid compliance with AML/ CFT requirements;

(c) cooperating and sharing information promptly with other competent domestic authorities, by requesting and providing assistance in investigations, prosecutions or proceedings relating to proceeds of crime, money laundering and terrorist financing;

(d) taking regulatory action against those institutions and persons regulated by it which fail to adequately comply with statutory AML/CFT obligations and Guidelines issued by the BOG;

(e) sharing of information with the FIU as required for the purposes of AML/CFT. This includes disclosing information to the FIU as soon as is reasonably practicable but no later than three working days after acquiring any information concerning suspicious transactions or activities that could be related to money laundering, terrorist financing or the proceeds of crime;

(f) maintaining statistics concerning measures adopted and sanctions imposed under the Act;

(g) developing standards and criteria applicable to the communication of suspicious activities that reflect other existing and future pertinent national and internationally accepted standards;

(h) ensuring that financial institutions as it relates to their foreign branches/subsidiaries implement and enforce standards consistent with the AML/CFT Act, Regulations, guidelines or directives. The BOG should be duly notified in cases

[9] Refer to Section 22 (1) of the AML/CFT Act 2009 and Section 13 of the AML/CFT Regulations 2010

where the foreign branches/subsidiaries are unable to implement and observe these standards; and

(i) sharing of information with agencies in other jurisdictions with similar functions as it relate to investigations, prosecutions pertaining to the proceeds of crime, money laundering, terrorist financing, and violations of the law and regulations dealing with financial institutions.

Regulatory actions[10] that could be taken by the BOG include:

(a) the issuance of written warnings;
(b) compliance orders with specific instructions;
(c) suspension, restriction or revocation of licence;
(d) prohibiting convicted persons from gaining employment within the sector;
(e) requesting regular reporting from the financial institution on the measures it is taking to comply with the law.

The BOG is required to inform the FIU as to the sanctions imposed and may publish its decision.

Section 2.2 is amended by inserting the following:

2.2.1 *SUPERVISION AND REGULATION OF FINANCIAL GROUPS*

2.2.1.1 Risk-Based Approach

The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions or groups will be determined on the basis of the ML/TF/PF risks. Greater monitoring resources will be directed to the financial institution's products, services and business relationships which present a higher risk than those presenting a lower risk. Financial institutions/groups must demonstrate to the BOG, that the extent of their CDD measures and monitoring is appropriate in view of their ML/TF/PF risk exposures.

[10] Refer to AML/CFT Act 2009 – Section 23 (1)
Refer to AML/CFT Act 2009 – Section 11 (1) & (2)

The following will be considered by the BOG when allocating resources for the monitoring of LFIs/groups:

a) size and complexity of the financial institution/group;

b) nature, scope and delivery channels of the products and services provided by the LFI;

c) most recently published National Risk Assessment;

d) the financial institution's risk assessment and findings; and

e) nature, scope and effectiveness of the financial institution's monitoring systems.

2.2.1.2 Foreign Branches and Subsidiaries

Where a financial institution has branches, subsidiaries, representative offices or are members of any financial group located in a country or territory outside of Guyana, it must communicate, implement and monitor group-wide AML/CFT/CPF programmes which must be appropriate to each category of institution. The programme must include:

a) policies and procedures for sharing information required to conduct CDD and ML/TF/PF risk management;

b) AML/CFT/CPF management procedures;

c) on-going training programmes for employees;

d) group-level compliance, audit which must include the appointment of a CO at the management level. The AML/CFT/CPF functions should be provided with the customer, account and transaction information from branches, subsidiaries, and representative offices when necessary for AML/CFT/CPF purposes;

e) monitoring of significant customer relationships and their transaction activities on a consolidated basis;

f) the different risk factors posed by each line of business and customer;

g) sharing of information on the identity of customers and their transaction activities within the group; and

h) adequate safeguards on the confidentiality and use of information exchanged including safeguards to prevent tipping-off.

In instances where the minimum AML/CFT/CPF requirements of the host country are less strict than those of the home country, financial institutions are required to ensure that their

branches, subsidiaries and representative offices in the host country implement the requirements of the home country to the extent that the host country's laws and regulations permit. Where the host country does not permit the effective implementation of the AML/CFT/CPF measures, the financial group must apply appropriate additional measures to manage the ML/TF/PF risks and inform the home supervisors.

If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group.

2.3 OTHER FORMS OF INTERNATIONAL COOPERATION

Efficient co-operation between foreign financial supervisors and their counterparts is aimed at facilitating effective AML/CFT/CPF supervision. Financial supervisors must therefore have a legal basis for providing co-operation, consistent with applicable international standards with respect to exchange of supervisory information for AML/CFT/CPF purposes.

Financial supervisors must also be able to exchange with foreign counterparts, information available domestically, including information held by financial institutions, and in a manner proportionate to their respective needs. There should be exchange of the following types of information for AML/CFT/CPF purposes, specifically with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:

a) *regulatory information, including information on the domestic regulatory system, and general information on the financial sectors.*
b) *prudential information for core principle supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and proper data;*
c) *information on internal AML/CFT/CPF procedures and policies of financial institutions, CDD information, customer files, samples of accounts and transaction information;*

Supervisors should be able to conduct inquiries on behalf of foreign counterparts, and where necessary, authorize or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate group supervision.

All dissemination of information exchanged for supervisory or non-supervisory purposes must be subject to prior authorization by the requested supervisor unless the requesting supervisor is under a legal obligation to disclose or report the information requested. In such cases, the requesting supervisor should inform the requested authority of his/her obligation. Prior authorization includes any deemed prior authorization under a Memorandum of Understanding.

2.3.1 Safeguards on Information Exchanged

Information exchanged must only be used for the purpose for which the information was sought/provided. Any dissemination of information to other authorities or third parties should be subject to prior authorization by the Bank.

Exchange of information must take place in a secure way and through reliable channels. The Bank may refuse to provide information if the requesting authority cannot effectively protect the information.

2.4 ENFORCEMENT OF THE GUIDELINE

Section 19 of the AML/CFT Regulations 2010 makes the failure to comply with the requirements of the Guideline a summary conviction offence. The Courts by Regulation 19 may also take account of the provisions of the Guideline in determining whether there has been compliance with the requirements of the AML/CFT Regulations. FIs are therefore advised to adopt the provisions of this Guideline and to implement the requisite internal systems and procedures.

2.5 LEGAL PROTECTION AND INDEMNIFICATION[31]

When a suspicious transaction or suspicious activity report is made to the FIU in good faith, financial institutions their employees, officers, directors, owners or other representatives as authorized by law, are exempted from criminal, civil or professional liability action as the case may be, or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, who in good faith transmit information or submits reports to the FIU regardless of the result of the communication.

2.5 TIPPING OFF[12]

Section 2.5 is amended by inserting the following:

If LFIs form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD or ongoing process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR. LFIs should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

It is an offence for employees, directors, officers or agents of a financial institution to disclose that a suspicious transaction report or related information on a specific transaction has been reported to the FIU; or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

In the event that a person is found guilty of tipping off he/she may, on conviction, be liable to a fine not exceeding one million dollars and to imprisonment for a term not exceeding 3 years.

[31] Refer to AML/CFT Act 2009 - Section 11 (1) & (2)

PART 5 – DUE DILIGENCE / HIGH RISK

5.1 CUSTOMER DUE DILIGENCE (CDD)

Customer due diligence is an essential element of the effort to prevent a financial institution from being used to perpetrate money laundering and terrorist financing.

CDD policies and procedures should however, not only be geared toward the timely prevention and detection of money laundering and terrorism financing activities, but must also form a fundamental part of the financial institution's overall risk management and internal control systems. It must contain a clear statement of management's overall expectations and establish specific lines of responsibilities not only at the point of the institution's first contact with the customer, but throughout the business relationship. Policies and procedures should be properly documented and clearly communicated to all relevant staff.

This is essential, as inadequate CDD standards can result in undue risk exposures, particularly as they relate to reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to financial institutions (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

As part of the due diligence process, a financial institution should:

(a) identify and verify a customer's identity using reliable, independent source documents, data or information prior to establishing a business relationship.

(b) identify the beneficial ownership and control structure of the customer and take reasonable measures to verify the identity of the existence of beneficial owners[47] and controllers such that a financial institution is satisfied that it knows who the beneficial

[47] "Beneficial owner" is defined in the FATF 40 Recommendations as a natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement over a legal person or arrangement.

owners and controllers are. That is, reliable and independent source documents must be provided when identifying and verifying the identity of the beneficial owners of legal persons.

(c) gather information on the nature of the customer's business, registered office and/or principal place of business, economic circumstances, purpose and intended nature of the business relationship. The extent of documentary evidence required will depend on the applicant and the nature of the applicant's business. Documentation confirming the nature of the applicant's business (e.g. audited financial statements) or the applicant's occupation (e.g. job letter or last pay slip) and source of funds to be used during the relationship should be provided.

(d) obtain information on the type, volume and value of the activity that can be expected within the relationship. Where major changes have been noted, an explanation should be sought from the customer for these changes.

Section 5.1 is amended by inserting the following:

Reliance on Third Party

In instances where reliance is placed on third party verification, the LFI must therefore obtain information on the level of the country risk in which the third party is based in order to determine whether the third party meets the requirements for performing the verification.

Once a business relationship has been established, ongoing due diligence on the business relationship and scrutiny of transactions should be undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile.

Section 5.1 is amended by inserting the following:

CDD for Beneficiaries of Life Insurance Policies

In addition to the CDD measures required for the customer and the beneficial owner, financial institutions are required to conduct the following CDD measures on the beneficiaries of life insurance policies and other investment related insurance policies, as soon as the beneficiary is identified or designated:

(a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout;

(c) for both the above cases – verifying of the identity of the beneficiary which should occur at the time of the payout. The payout to a beneficiary of a life insurance policy is not an occasional transaction but is the result of the business relationship into which the service provider has entered with the policyholder. If the beneficiary of a life insurance policy is a legal entity, the beneficial owner of that legal entity needs also to be identified and his/her identity verified, using risk-based and adequate measures; and

(d) taking measures to determine whether the beneficiary or the beneficial owner of the life insurance policy is a PEP. This should occur, at the latest, at the time of the payout. Where higher risks have been identified, in addition to performing normal CDD measures, financial institutions should:

(i) inform senior management before the payout of the policy proceeds; and

(ii) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider filing a STR if the financial institution is unable to comply with the above information.

5.2 ENHANCED DUE DILIGENCE (EDD)

Financial institutions are required to perform enhanced due diligence for higher risk customers. Such measures shall be on a risk sensitive basis for categories of customers, business relations or transactions as the financial institution may assess to present a higher risk for money laundering or terrorist financing. A financial institution may conclude, under its risk based approach, that a customer is high risk because of the following:

(i) customer's business activity;

(ii) ownership structure;

(iii) nationality;

(iv) residence status;

(v) countries the customer is doing business with. A financial institution may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries. In some cases it may be necessary to refuse the business relationship from the inception because of the higher risk involved;

(vi) anticipated or actual volume of transactions;

(vii) types of transactions.

The extent of additional information sought and any monitoring carried out in respect of any particular customer or class/category of customer, will depend on the money laundering or terrorist financing risk that the customer poses to the financial institution and the product or service being sought that carries a higher risk of being used for money laundering or terrorist financing purposes. The financial institution's policy framework should therefore include a description of the types of customers that are likely to pose a higher than average risk and procedures for dealing with such applications.

A financial institution should give particular attention to the following business relations and transactions:

(i) where a customer has not been physically present for identification purposes; correspondent relationship;
(ii) a business relationship or occasional transaction with a PEP;
(iii) business relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML/CFT measures;
(iv) corporate customers able to issue bearer shares or bearer instruments;
(v) cash transactions in excess of two million dollars.

In addition the reporting institution should establish internal criteria (red flags) to detect suspicious transactions. The reporting institution should be prompted to conduct enhanced

due diligence if any transaction matches the red flags list. Transactions that match the red flags should be subject to on-going monitoring

5.3.8 Politically Exposed Persons (PEPs)

Section 2 (1) of the AML/CFT Act 2009 defines a "Politically Exposed Person" or PEP as any individual who is or has been entrusted with prominent public functions on behalf of a state, including a Head of State or of government, senior politicians, senior government, judicial or military officers, senior executives of state owned corporations, important political party officials, including family members or close associates of the politically exposed person whether that person is resident in Guyana or not.

PEP status itself does not automatically mean that the individual is corrupt or has been incriminated in any corruption. However, their office and position can leave them vulnerable to corruption. The risks increase when the person concerned is from a country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards, or where these do not meet international financial transparency standards.

Business relationships with individuals holding important public positions and with the immediate family members of PEPs or companies in which the PEP is the beneficial owner may expose financial institutions to significant reputational, legal risk and costly information requests and seizure orders from law enforcement or judicial authorities. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud.

Furthermore, public confidence in the ethical standards of a whole financial system can be undermined since such cases can receive extensive media attention and strong political and public reaction, even if the illegal origin of the assets is often difficult to

prove. As such, a financial institution should conduct enhanced due diligence where it has determined that an applicant for business is a PEP.

To mitigate the significant legal and reputational risk exposures that financial institutions face from establishing and maintaining business relationships with PEPs, due diligence procedures such as outlined below should be followed prior to the commencement of such relationships:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;

(b) obtain the senior management's approval before establishing such business relationships;

(c) take reasonable measures to establish the source of wealth/property/funds in accordance with Section 15(4)(d)(iv) of the AML/CFT Act, 2009 .

(d) develop policies, procedures and processes such as the use of electronic databases and publicly available information to assess whether a customer is or has become a PEP.

In addition to the identity information normally requested for natural persons, for PEP information on immediate family members or close associates having transaction authority over the account should be obtained.

Section 5.3.8 is amended by inserting the following:

In cases of domestic PEPs or persons who have been entrusted with prominent functions by an international organization, financial institutions should undertake a risk assessment of the PEP's business relationship. This should be an overall assessment of all risk factors needed to determine whether the business relationship with the PEP is of higher risk.

The risk assessment must take into account the customer, country, product/service and transaction or delivery channel risk factors. Additional factors including the nature of the prominent public function that the PEP has, such as his/her level of seniority, access to or control over public funds and nature of positions held.

If the risk assessment establishes that the business relationship with the domestic PEP presents a low level of risk, then the institution should apply standard CDD measures and monitoring. However, where the relationship poses a higher risk, then the institution is required to apply the enhanced due diligence measures consistent with those of foreign PEPs/other high-risk customers.

Foreign PEPs

LFIs must have the appropriate risk management systems to determine if a customer or beneficial owner is a foreign PEP, the system implemented should be dependent on the nature of the institution's business, nature of its client's profile, expected transactions and other risk factors.

Foreign PEPs must always be considered high-risk and require application of enhanced due diligence measures on an ongoing basis as for all higher risk customers.

Following the commencement of banking relationships, there should be:

(a) enhanced due diligence of the business relationship with regular review by the Compliance Officer or senior management using a risk-based approach, at least yearly, with the results of the review duly documented;
(b) close scrutiny of any complex structures e.g. involving legal structures such as corporate entities, trusts, foundations and multiple jurisdiction established by the PEP;
(c) close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer negotiable instruments which break an audit trail, the use of unknown financial institutions and regular transactions involving sums just below a typical reporting level;
(d) close scrutiny of transactions requested by the PEP that are unexpected given
(e) the customer's account profile;
(f) close scrutiny of amount and transaction which do not make sense given the
(g) PEP's known income source and uses;

(h) close scrutiny of transaction which exceeds reasonable amounts in relation to the PEP's known net worth.

The financial institution should regularly review and maintain a current listing of PEPs.

Financial institutions should not establish business relationships with PEPs if the financial institution knows or has reason to suspect that the funds are derived from corruption or misuse of public assets.

Whilst it is appreciated that efforts must be made to protect the confidentiality of PEPs and their businesses, these accounts must be available for review by the BOG, the FIU, Law Enforcement Authorities where required, and external auditors.

5.4.3.2 Cross –border Wire Transfers

(1) Remitting Financial Institution

Financial institutions that initiate wire transfers on behalf of customers to a beneficiary overseas must ensure that the customer's information conveyed in the payment message or instruction is accurate and has been verified. Verification of the identity of the originator/customer should be done before conducting any funds transfer or one-off (i.e. occasional) transactions with customers and should include the following requirements.

Section 5.4.3.2 is amended by inserting the following:

Additionally, financial institutions are required to ensure that all cross-border wire transfers above USD/EURO 1,000 are always accompanied by:

(i) the identity of the originator/remitting customer (including name and address, official identification information)
(ii) the name and address of the ultimate recipient/beneficiary
(iii) related narrative /instructions that accompany transfers
(iv) amount and currency type should be clearly stated
(v) routing number if applicable
(vi) execution date of the payment order
(vii) identity of the beneficiary' financial institution

(viii) Account number of the beneficiary where such an account is used to process the transaction. In the absence of an account number, any other unique transaction reference number may be included.

The payment message should be signed by the customer or the authorized signatories on the account and authenticated.

The above shall not apply to wire transfers/settlements between financial institutions where the originator and beneficiary of the funds transfer are acting on their own behalf.

Section 5.4.3.2 is amended by inserting the following:

Where several individual wire transfers from a single originator are bundled in a batch file for transmission to multiple beneficiaries, there is no need for originator information for each transfer within the batch file provided that:

(i) the batch file contains complete originator information;

(ii) the individual transfer includes the account number of the originator;

(iii) there is full beneficiary information that is fully traceable within the beneficiary country.

Where any de minimus thresholds are applied in relation to any cross-border transfer at (1) above, financial institutions are required to ensure that such transactions below any applicable de minimus thresholds (no higher than USD/EURO 1,000) are always accompanied by originator and beneficiary information as specified below:

(a) Required originator information:

(i) the name of the originator; and

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction

The ordering financial institution shall not execute the wire transfer where it is unable to collect and maintain information on the originator or beneficiary.

The ordering financial institution shall adopt effective risk-based procedures capable of detecting missing and/or incomplete information for both the originator and beneficiary from the payment and settlement system used to effect the transfer of funds. It is the expectation that monitoring should not be undertaken at the time of processing the transfer in order to avoid disruption of straight-through processing.

The ordering financial institution shall consider missing or incomplete information on the originator as a risk factor in assessing whether the transfer of funds or related transaction is suspicious and whether it must be reported to the FIU.

In cases where the financial institution controls both the originator and beneficiary sides of a wire transfer, the financial institution must:

(i) take into account all information from both the originating and beneficiary sides in order to determine whether a STR should be filed; and

(ii) file a STR in any country affected by the suspicious wire transfer and make the relevant information available to the FIU.

5.4.3.3 Domestic Wire Transfer

Financial institutions must ensure that information accompanying domestic wire transfers include originator information similar to that required for cross-border wire transfers, unless the information can be made available to the beneficiary financial institution and the appropriate authorities by other means. In such instances, the originator institution should only include the account number.

The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following:

(i) the customer address;

(ii) a national identity number or a date and place of birth; and

(iii) transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities.

SG No. 13 is amended by inserting the following:

PART 9 - PROLIFERATION FINANCING

ACRONYMS

Acronym	Translation
AML	Anti-money Laundering
CFT	Countering the Financing
CPF	Countering Proliferation Financing
EDD	Enhanced Due Diligence
ML	Money Laundering
TF	Terrorist Financing
PF	Proliferation Financing
WMD	Weapons of Mass Destruction
LFI(s)	Licensed Financial Institution(s)
FATF	Financial Action Task Force
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolutions
TFS	Targeted Financial Sanctions
DPRK	Democratic People's Republic of Korea

I. INTRODUCTION

1. This amendment to Supervision Guideline (SG) No. 13 on proliferation financing is being issued to licensed financial institutions (LFIs) so that they may guard against the threat of proliferation financing (PF). It also raises the awareness of PF threats, vulnerabilities, and risks and highlights the relevant requirements for LFIs. It encompasses the domestic legislative requirements and international standards and obligations relevant to combatting proliferation financing.

2. The identification, assessment, understanding and management of PF risk are key to a robust AML/CFT regime and all LFIs must include countering PF (CPF) in their AML/CFT programme and risk management strategies.

3. PF is "the act of providing funds or financial services which are used, in whole or in part for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or where applicable international obligations"[5].

This amendment is applicable to all LFIs regulated and supervised by the Bank.

II. PF THREATS AND VULNERABILITIES

4. PF threats are mainly external and are in relation to foreign state and non-state actors attempting to exploit LFIs to finance, procure, ship/trans-ship goods for use in the proliferation of weapons of mass destruction (WMD). Traditionally, the most active PF threats were posed by states seeking to obtain or expand capabilities in relation to nuclear weapons and other WMDs. However, the current priority threats are:

- *State actors* - listed countries have created global networks of shell/front companies and employ complex, deceptive measures to conceal their PF activities and evade international sanctions levied against them.

[5] The 2010 FATF Status Report on Combatting Proliferation Financing

- *Non-state actors* - terrorist groups that have targeted countries for fundraising and have a stated intent to pursue nuclear weapons and radiological materials.

5. LFIs must be aware that the absence of direct links to listed countries or non-state actors does not necessarily mean that a transaction or customer is low-risk since proliferators have been able to hide their involvement and nature of activity underlying a transaction.

6. Factors which contributes to a high PF vulnerability include:
   - illicit commercial and financial links with high-risk jurisdictions;
   - insufficient understanding, awareness, and expertise of PF risk; and
   - weaknesses in shipping and transshipment controls, including transparency, monitoring capabilities or other discrepancies in trade finance requirements; and
   - insufficient familiarity with the list of dual use goods for monitoring.

III. INTERNATIONAL STANDARDS AND OBLIGATIONS TO COUNTER PF RISK

7. This amendment is in accordance with the requirements of the Financial Action Task Force (FATF) Recommendation 7 and the United Nations Security Council Resolution (UNSCR) 1540 and Section 13 (68E) (12) of the AML/CFT (Amendment) Act No. 17 of 2018 and the AML/CFT Regulation No. 10 of 2023.

8. Further, the relevant mechanisms are also in place with other domestic competent authorities to cooperate and coordinate in relation to the development and implementation of policies and activities to combat ML, TF and PF in accordance with FATF Recommendation 2.

RECOMMENDATION 7

9. The recommendation requires that countries implement targeted financial sanctions prescribed by the United Nations Security Council Resolutions (UNSCR) related to the proliferation of WMD and the financing of proliferation. The implementation of the resolutions requires that countries freeze without delay:

- all funds and other assets which are owned and controlled by designated persons/entities and not just those that can be tied to a particular act, plot or threat of proliferation;
- all funds or assets that are wholly or jointly owned or controlled directly or indirectly by designated persons or entities;
- funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities; and
- funds or other assets of persons and entities acting on behalf of or at the direction of, designated persons or entities.

10. The recommendation also requires that institutions implement preventative measures to counter the flow of funds or assets to those who are responsible for the proliferation of weapons of mass destruction. The recommendation is not risk-based and is applicable to all existing and future successor resolutions and are relevant to two country-specific regimes, DPRK and Iran.

11. All LFIs must screen names and addresses of all customers against lists of designated persons and entities, including entities owned or controlled by them published by the UN Security Council or its committees in order to ensure compliance with TFS and are applicable to persons/entities designated by the UN Security Council or relevant committees based on the following criteria:
    - Persons/entities engaging in or providing support for, including through illicit means, proliferation sensitive activities and programmes;
    - Persons/entities acting on behalf of or at the direction of designated persons/entities;
    - Persons/entities controlled by designated persons/entities; and
    - Persons/entities assisting designated persons of entities in evading sanctions, or violating resolution provisions.

12. Under this recommendation, all LFIs are required to implement measures to identify, and detect persons, entities, and transactions relevant to PF. These measures include ensuring that the targeted financial sanctions are implemented effectively, without delay, robustly, prevent prohibited payments, and preserve the rights of the innocent third parties.

UNSCR 1540

13. On April 28, 2004 the UNSC adopted UNSCR 1540, which was established to prevent non-state actors from acquiring nuclear, biological, and chemical weapons, their means of delivery, and related materials. The resolution filled a gap in international law by addressing the risk that terrorists might obtain, proliferate, or use WMDs.

14. The UNSCR 1540 imposed the following three (3) primary obligations in an effort to restrict PF. The financial provisions of the Resolution require that all States:
    - abstain from supporting non-state actors seeking WMDs and their means of delivery;
    - adopt and implement effective laws (i.e. criminal or civil penalties for violations of export control laws) to prohibit non-state actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their means of delivery; and
    - establish and enforce effective measures and domestic controls (i.e. export and transshipment controls) to prevent the proliferation of nuclear, chemical, or biological weapons, their means of delivery and related materials.

15. Additionally, the UNSC has adopted another approach to counter PF through resolutions made under Chapter VII of the UN Charter and thereby imposing mandatory obligations for UN Member States. Articles 39 through 51 detail obligations in relation to addressing all threats to global peace, employing armed or military forces should threats occur, implementing preventative measures to combat these threats and restoring and maintaining international peace.

IV. RISKS ASSOCIATED WITH PF

16. During the risk assessment, LFIs must take into consideration the following which could be indicators of increased PF risks:

    i. ***Proliferation Risk*** - does not only relate to countries at high-risk of PF. Countries and terrorist groups also rely on transnational connections to produce illicit good and services. For example, the DPRK ***relies*** extensively on corporate networks in China, Hong Kong, Singapore and Malaysia.

    ii. ***Country/Geographic Risks*** - LFIs must assess whether the customer is located in a country that is subject to a ***relevant*** UN sanction (i.e. DPRK or Iran) or is listed on a National Listing[6] for high risk entities;

    iii. ***Product/Service Risk*** - determine whether the specific products/services offered by the LFI could involve potential proliferation factors, for example, delivery of financial services such as trade financing, correspondent banking to a country targeted on the EU or UN Sanctions Listing).

    iv. ***Customer Risk*** - upon opening of accounts, and when conducting ongoing due diligence, LFIs must ascertain the type of business the customer is engaged in order to assess whether it poses potential proliferation risks, for example, if the client is involved in the export trade, then assess whether the client is involved in transactions with end-users who are listed on a National Listing. LFIs must also determine whether the customer's end-user is associated with a listed military or research company connected with a high-risked jurisdiction which may be of PF concern.

17. The following variables specific to the customer and transactions must also be considered:

    - duration of relationship;
    - purpose of relationship;
    - whether the customer seeks to obscure their interest through family members or close business and other associates;

[6] United Kingdom/European Union Specially Targeted List or Office of the Foreign Asset Control Listing

- in case of higher-risk customers, LFIs should consider lowering the ownership and control threshold to identify additional beneficial ownership interests;
- corporate structure;
- volume of anticipated transaction; and
- making risk-based decision whether the institution is willing to accept customers in which a designated person has a non-controlling interest.

18. In addition, customers and entities that produce sensitive goods, dual use goods, or companies involved in advanced research can also pose PF risk to the LFI. For example:
    - shipping companies serving high-risked regions;
    - customers who produce dual use goods may not be familiar with the rules governing export and customers who are unaware of the need to implement their own PF safeguards; and
    - customer who use shell and front companies to disguise end users and payments.

19. ***Trade finance transaction*** involving controlled goods or technology presents a higher level of PF risk. The complexity of these transactions can allow individuals and entities to hide their illicit activities. Both traditional document based trade finance transactions and cross-border wire transfers related to trade finance can pose high PF risk.

20. ***Cross border wire transfers*** involve great PF risk since they often include less information on the underlying activity making it more difficult for LFIs to understand the transaction. Wire transfers are also processed easier than traditional trade financing instruments such as letters of credit and performance bonds which usually involve more extensive due diligence and documentation.

21. ***Correspondent Banking services*** are also a significant source of PF risk since activities such as clearing intermediary wires can pose risk to the LFI because the institution must process transactions for the customers of the LFI's customers. This risk is elevated when the correspondent banking relation exposes the LFI to a region with links to PF.

22. ***Delivery Channel Risk*** - LFIs are required to consider the channels used to take on new customers and how those customers are accessing products and services. Special focus should be on the channels not normally used or those that are not in line with the normal behavior pattern of customers.

V. MANAGEMENT OF PF RISKS

23. LFIs must include CPF in their AML/CFT programmes, as well as their group-wide programme where applicable. In addition, the risk-based approach to managing the PF risk to which the institution is exposed must also be included in the compliance programmes. Appropriate risk management strategies which incorporate controls to mitigate the PF risk inherent in their AML/CFT structure must also be implemented.

24. This can be achieved through:

- applying objective criteria to assess the potential PF risk by using the institution's expertise and obtaining information from governmental agencies;
- building on the LFI's existing AML/CFT framework by incorporating PF risk factors for consideration along with wider determination of risk factors;
- using the institution's established mechanism to conduct risk assessments and identifying suspicious activity that is applicable to PF;
- implementing risk-based anti-proliferation financing policies and procedures, comparable to international standards, including training to identify suspicious transactions; and
- developing and maintaining relevant in-house policies and procedures relative to countering PF and complying with PF guidelines.

25. When introducing PF into an institution's existing risk assessment, the practice should be proportionate to the overall proliferation risk associated with the activities currently being undertaken by the institution.

EDD

26. LFIs must conduct EDD on higher risk transactions and entities. Lists which are compiled by national authorities must be used to assist the institution since they provide information on entities and individuals who may pose a proliferation concern.

27. EDD should focus on obtaining information in relation to expected customer behaviour, with special focus on the expected end user of any sensitive products and the customer's expected exposure to high-risked jurisdictions, including transhipment hubs.

28. LFIs must also apply EDD to transactions involving any proliferation-sensitive goods or services, regardless of whether or not the customer is high-risk. At on-boarding special attention should be paid to identifying the end-user of the sensitive goods.

29. Customers must also be required to provide a valid export license for individual transactions or reference to the export control requirements of the relevant jurisdiction to indicate that the exported goods do not require a permit.

CUSTOMER SCREENING

30. LFIs must screen the entire customer base including beneficial owners, authorised signatories and addresses, whenever a new designation is announced. All new customers being on-boarded must also be screened prior to on-boarding. Screening must also be done prior to entering into the transaction for all walk-in customers who engage in one-off transactions.

31. In addition to screening customers, all LFIs must also ensure that they comply with the requirement to freeze all funds that the designated person controls both directly and indirectly. LFIs must also conduct the appropriate due diligence to ensure that they know their customers and whether they are controlled by a third party.

32. A real-time sanctions screening system must also be in place for all incoming and outgoing payments which must be capable of identifying a match against all lists maintained by the

LFI. If a match is found it must be put on-hold until the transaction is reviewed by the appropriate authority in the institution.

33. All screening lists maintained by LFIs must be updated immediately upon receiving notice of a designation. In the event that an LFI uses a screening list provided by a third party vendor, the vendor's service level agreement with the LFI must ensure that the screening list is updated within 24 hours of a new updated designation being issued.

34. Transactions screening and monitoring systems must be capable of screening and monitoring all aspects of customer onboarding and payment messages, including all information provided by the ordering customer/institution.

35. Information on all the relevant terms, such as dual use goods, jurisdictions subject to sanctions, and major ports and cities within those jurisdictions must be maintained on the LFIs sanctions screening lists.

VI. FREEZING OF ACCOUNTS

36. When implementing targeted financial sanctions LFIs must place a restriction on any account meeting any of the following criteria:

- the account represents funds or other assets that are owned or controlled by the designated person or entity, beyond those that can be tied to a particular act, plot or threat of proliferation;
- the account represents funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities;
- the account represents funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities; and
- the account represents funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

VII. HOLDING/STOPPING TRANSACTIONS

37. All outgoing and incoming transfers must be screened in real-time and transactions must be monitored to detect any transactions that must be stopped to take any further actions as necessary. If a customer seeks to make a transfer or carry out a transaction to an individual or entity subject to UN sanctions, the LFI must immediately, if a match is identified:
    - hold the funds that would have been subject to the transfer and/or transaction;
    - file an STR; and
    - inform the relevant supervisory authorities.

38. The funds must not be returned to the customer and should remain with the LFI until the competent authorities have carried out a full investigation into the purpose of the payment and the nature of the customer's relationship with the designated person. LFIs must comply with the directions of the supervisory authority regarding ultimate disposition of the funds. LFIs should under no circumstance provide the customer with any information indicating that an STR has been filed.

VIII. REPORTING

39. LFIs are required to immediately implement a designation order, and report any actions taken in compliance with the designation to the relevant supervisory authorities within 48 hours of issuance of the designation order. This include:
    - any accounts frozen;
    - any transactions stopped, on-hold, or blocked;
    - all screening performed; and
    - any other efforts to comply with sanctions.

40. Institutions must report again to the relevant supervisory authorities within 30 days after issuance of the designation order whether or not they have taken any additional actions.

41. Once the above reports have been made, the institution is required to report if they have frozen any additional accounts/funds or blocked any transactions. Account and/or customer relationship should be subject to enhanced monitoring as well.

IX. FALSE POSITIVES

42. List-based screening may result in hits/detections where a person related to an account or transaction has the same name or the same address as a designated person. LFIs are required to take a conservative approach to sanctions hits, that is, they cannot assume that a hit is a false positive but must thoroughly investigate every hit.

43. Generally, in such an investigation, LFIs must compare information that is known about the party in question, such as date of birth and address, with other information provided in the designation order. If the party in question is not a customer, the LFI may need to request that the customer provide reliable proof of its counterpart's identity, such as a copy of a government-issued photo identification document. If the LFI identifies information that establishes that the party in question is not a designated person, then the LFI does not need to block the transaction or hold the account.

44. Detailed records should be kept of the process followed, the evidence obtained, and the rationale for releasing a transaction. To avoid duplicative investigations, LFIs may create a "false hit list" along with records of customers that have the same name as designated persons and whom the LFI has determined, after a thorough investigation, not to be the person that has been designated. This list can be used to update the monitoring software in order not to place alerts on such matches. Notwithstanding that this practice is acceptable, it carries an element of risk. Therefore LFIs should regularly review and update the list to ensure that authentic matches are not suppressed. The list must be subject to independent or external audit periodically.

45. In instances where LFIs are approached by persons who claim that their funds/accounts have been mistakenly frozen due to them sharing the same name with a designated person, such claims must be thoroughly investigated using the same process as used for hits from automated monitoring systems. If there are doubts about the identity of the claimant, the LFI should refuse to unfreeze the funds and allow the claimant to pursue legislative remedies.

X. UNFREEZING

46. Unfreezing generally only takes place when a when a formerly designated person is no longer designated.

47. In rare circumstances, designations may be rescinded. For example, a designated person may cease to be involved in proliferation activities and therefore be removed from UN sanctions list. LFIs may receive court orders, to unfreeze funds and accounts for certain purposes. LFIs should seek guidance from the Director of Public Prosecution and the relevant supervisory authority in instances where there are any questions about compliance with such orders.

48. Institutions must continue to monitor updates to the relevant sanctions list so that they are aware if a person has been de-listed. Unfreezing should take place promptly but with appropriate due diligence and deliberate caution, consistent with the terms of de-listing and any guidance from supervisory authorities. LFIs must continue to be vigilant to ensure that accounts or funds are not transferred to other designated persons.

XI. PENALTIES

49. Since freezing of accounts or transactions is a consequence of a designation order, failure to comply with these requirements can lead to extremely high fines and even a prison term.

50. Section 13 (68E) (12) of the AML/CFT (Amendment) Act No. 17 of 2018 provides for strict penalties for failure to comply with the legal requirements regarding freezing of funds or other assets related to a listed person or entity. It states that:

> *"a natural person who commits this offence shall be liable on summary conviction to a fine of not less than five million dollars nor more than one hundred millions dollars or to imprisonment for up to seven years and in the case of a body corporate to a fine of not less than ten million dollars nor more than two hundred million dollars."*

XII. RED FLAGS AND TYPOLOGIES OF POTENTIAL PF RISKS

51. Red flags for PF risks under the following indicators include, but are not limited to:

CUSTOMER

- the customer or counter-party, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists;
- customer is a military or research body connected with a higher risk jurisdiction of proliferation concern.
- the customer's activities do not match the business profile;
- the customer is vague about the end-user(s) and provides incomplete information or is resistant when requested to provide additional information;
- a new customer requests a letter of credit from a LFI, whilst still awaiting approval of its account; and
- the customer uses complicated structures to conceal involvement, for example, uses layered letters of credit, front companies, intermediaries and brokers.

TRANSACTIONS/ ORDERS

- the transaction concerns dual-use, proliferation-sensitive or military goods, whether licensed or not;
- the transaction involves an individual or entity in any country of proliferation concern;
- the transaction reflects a link between representatives of companies (e.g. same owners or management) exchanging goods, in order to evade scrutiny of the goods exchanged;
- the transaction involves the shipment of goods inconsistent with normal geographic trade patterns i.e. where the country involved does not normally export or import the types of goods concerned; and
- the order for goods is placed by firms or individuals from countries, other than the country of the stated end-user.

JURISDICTIONS

- countries with weak financial safeguards and which are actively engaged with a sanctioned country;
- the presence of an industry that produces dual-use goods, proliferation-sensitive items or military goods;
- deliberate insertion of extra links into the supply chain;
- countries that are known to have weak import/export control laws or poor enforcement; and
- countries that do not have the required level of technical competence in regard to certain goods involved.

OTHER

- project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user;
- declared value of shipment under-valued in relation to shipping cost;
- inconsistencies in information contained in trade documents and financial flow e.g. names, addresses, final destination;
- the use of fraudulent documents and identities e.g. false end-use certificates and forged export certificates;
- the use of facilitators to ensure the transfer of goods avoids inspection;
- freight forwarding firm being listed as the product's final destination;
- wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation; and
- pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

XIII. TYPOLOGIES OF THE FINANCING OF POLIFERATION RISKS

52. **The Khan Case** - consists of several different proliferation cases over a long period, concerning nuclear weapon programs in several jurisdictions of proliferation concern. The process of proliferation for each item to be constructed consisted of many steps in order to disguise the activities of the network and the true nature and end-use of the goods. Many individuals, companies and countries were knowingly or in good faith involved. Although some operations appear to have been settled in cash, others were settled through international transfers within the framework of duly established contracts. Contracts appeared to have been financed conventionally, through letters of credit or bills of exchange. Additionally, there were cash transactions within the network of customers. Amounts were deposited in bank accounts of emerging or offshore countries before transactions were made between banks for final beneficiaries.

53. **Proliferator A** - set up front companies and used other intermediaries to purchase magnets that could be used for manufacturing centrifuge bearings. Front Company #1 signed documents with the foreign jurisdiction's manufacturing company concerning the manufacturing and trade of magnets, however, it was not declared in these documents, nor was it detected by authorities, that these components could be used to develop WMD. The magnets were then transshipped to a neighboring third jurisdiction to Front Company #2. This jurisdiction is used as a "turntable" for goods, which means that goods are imported and re-exported. The proliferator used an intermediary to arrange the import and export to the third jurisdiction. The intermediary had accounts in the third jurisdiction and used his accounts to finance the acquisition of the goods and to launder the illegal funds used for these transactions. A combination of cash and letters of credit were used to pay for the trade of the magnets which totaled over USD 4M.

54. **Trading Company B** - in country Z deals in laboratory test-equipment for university and research centers and also for the energy sector. It is known to have procured dual-use items for country Z's WMD programs. Company B has bank accounts in a number of countries and has a UK account with a UK bank in country U, a known diversionary destination.

55. **R. David Hughes** - was the president of an Olympia, Washington-based company, AMLINK. AMLINK was a medical supply company, but was involved in export of commodities that did not match its business profile. In June 1996, the U.S. Customs Service began an investigation of the exportation of nuclear power plant equipment by Hughes and AMLINK from the Port of Seattle to Cyprus. The nuclear power plant equipment was to be shipped from Cyprus to Iran via Bulgaria, in violation of the U.S. embargo on Iran. Payment was made via wire transfer from Abi-Saad into Hughes U.S. bank account; Hughes then paid for the equipment with a cashier's check. The declared value of the shipment was under-valued. Hughes was indicted and convicted of export of nuclear equipment without a license.