BANK OF GUYANA

AMENDMENTS TO SUPERVISION GUIDELINE (SG) NO. 12

SG No. 12 is now amended as follows:

1. Part 4 - Enhanced Due Diligence is amended to include Cross-border Wire Transfers
2. Removal of paragraph 139- Proliferation Financing (PF)
3. Part 6 paragraph 140 is renumbered as 139
4. Part 6 paragraph 141 is renumbered as 140
5. Insertion of paragraph 141 – PF

SUPERVISION GUIDELINE NO. 12

PART 4 – ENHANCED DUE DILIGENCE

SPECIAL IDENTIFICATION REQUIREMENTS APPLICABLE TO MONEY TRANSFER AGENCIES

Part 4 is amended by inserting the following:

Cross-border Wire Transfers

61. Information should remain with the transfer or related messages through the payment chain. For cross-border transactions, MTAs are required to obtain and maintain accurate and meaningful information of:

- the name of the originator;
- the originator's reference number where such an account is used to process the transaction;
- the originator's address, national identification card or passport number and date of birth;
- the name of the beneficiary; and
- the beneficiary's account number 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.*

62. *Additionally, MTAs are required to ensure that all cross-border wire transfers above USD/EURO 1,000 are always accompanied by:*
    - *clearly stated amount and currency type;*
    - *routing number if applicable;*
    - *execution date of the payment order; and*
    - *identity of the beneficiary' MTA.*

63. *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.

64. Where any de minimus thresholds are applied in relation to any cross-border transfer, MTAs 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

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

66. The ordering MTA 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.

67. The ordering MTA 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.

68. In cases where the MTA controls both the originator and beneficiary sides of a wire transfer, the MTA 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 countries affected by the suspicious wire transfer and make the relevant information available to the FIU.

69. For domestic wire transfers, however, the ordering MTA must include full originator information or only the originator's account number or unique reference number, provided full originator information is available to the recipient MTA and competent authorities.

70. The customer identification number must refer to a record held by the originating MTA 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 MTA within three business days of receiving the request either from the beneficiary MTA or from appropriate competent authorities.

MONITORING OF TRANSACTIONS EDD

71. MTAs and Cambios may set limits for any category of transactions and pay particular attention to the transactions which exceed these limits. High-risk transactions have to be subjected to EDD. Key indicators shall be established for such transactions, taking note of the background of the customer, e.g., the country of origin, SOF, the type of transactions involved and other risk factors. A system of periodical review of risk categorization of customers shall be put in place and the need for applying EDD measures. MTAs and Cambios shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from countries classified by the FATF as uncooperative or high-risk countries that do not sufficiently apply the FATF Standards.

Suspicious Transaction Report (STR)

72. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined and written findings together with all the documents should be retained and made available to the FIU. Where MTAs and Cambios are unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, they shall not undertake the transaction. Under these circumstances, the MTA and Cambio shall file a STR with the FIU even if the transaction was not processed.

141. 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

This amendment to Supervision Guideline (SG) No. 12 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.

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.

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"[1].

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

II. PF THREATS AND VULNERABILITIES

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.

[1] 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.

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.

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

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.

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

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.

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.

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.

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

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.

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.

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

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[2] 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.

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;

[2] 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.

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.

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.

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.

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.

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

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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.

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.

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

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

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.

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

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.

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.

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

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.

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.

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.

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

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

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.

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

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.

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

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

Case Study 1

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.

Case Study 2

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.

Case Study 3

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.

Case Study 4

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.