GUIDELINE FOR TRUST AND COMPANY SERVICE PROVIDERS

NO. 3 OF 2023

JUNE 2023

(UPDATED AUGUST 2023)

Issued by the Antimoney Laundering/Countering the Financing of Terrorism/Proliferation Financing National Coordination Committee

TABLE OF CONTENTS

INTRODUCTION

Trust and Company Service Providers (TCSPs) conduct activities that are subject to regulation under the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009, as amended, (AMLCFT Act 2009).

These guidelines have been developed for the benefit of TCSPs and persons who may seek to become licensed as a TCSP. These guidelines also further highlight risks TCSPs may face, including sanctions evasion, illicit financing activities and other financial crimes. Additionally, these guidelines are geared towards assisting TCSPs in the implementation of a risk-based approach in applying measures to mitigate against Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) Risks.

This guideline reinforces the provisions of the AMLCFT Act 2009, Anti-Money Laundering and Countering the Financing of Terrorism Regulations, and the Guyana Compliance Commission Act.

The Financial Action Task Force (FATF) Guidance for a Risk-Based Approach for Trust and Company Service Providers has been factored into the development of these Guidelines. All TCSPs are guided to keep up to date with this publication and future publications from FATF that may be relevant to the sector.

Comprehensive AML/CFT Compliance by TCSPs and other regulated entities operating in or from within Guyana, also requires reporting and engagement with the Financial Intelligence Unit, Supervisory Authorities and competent authorities appointed under the AMLCFT Act 2009, including Law Enforcement Agencies, such as the Special Organized Crime Unit of the Guyana Police Force.

TCSPs face unique risks from bad actors who may seek to use TCSPs for ML/TF/PF.

APPLICATION

Applicable Persons to whom these Guidelines apply.

Section 2 of the AMLCFT Act 2009 provides that a reporting entity means any person whose regular occupation or business is the carrying on of-

(a) Any activity listed in the First Schedule; or
(b) Any other activity defined by the Minister responsible for Finance as such by an order published in the Gazette amending the First Schedule;

As per the First Schedule of the AMLCFT Act 2009, under 'Activities and businesses subject to the act, includes trust or company service providers, it provides:

> *"A trust or company service provider not otherwise covered by this definition which as a business, provide any of the following services to third parties as covered under the law relating to Trusts under the Civil Law of Guyana Act-*
>
> *(i) Acting as a formation agent of legal persons;*
> *(ii) Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;*
> *(iii) Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;*
> *(iv) Acting as (or arranging for another person to act as) a trustee of an expressed trust;*
> *(v) Acting as (or arranging for another person to act as) a nominee shareholder for another person."*

Pursuant to the **Fourth Schedule of the AMLCFT Act 2009** and the First Schedule of the Guyana Compliance Commission Act, the supervisory authority for Trust or Company Service Providers is the Guyana Compliance Commission.

Section 35 of the Guyana Compliance Act (GCC Act) provides that every reporting entity designated to be supervised by the Guyana Compliance Commission shall register with the Commission. This includes every reporting entity established before the coming into force of the GCC Act or established after the coming into force of the GCC Act, which fails to register within three (3) months of the commencement of business.

Pursuant to the First Schedule of the Guyana Compliance Commission Act which contains a list of the reporting entities of the Commission provides:

"Non-Financial Trust and Company Service Providers not otherwise covered by this definition, which as a business, provides any of the following services to third parties:

(a) formation agent of legal persons;

(b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

(d) acting as or arranging for another person to act as a trustee of an express trust; or

(e) acting as or arranging for another person to act as a nominee shareholder for another person."

These Guidelines are relevant for all persons operating as TCSPs in or from within Guyana. Any entity wishing to provide company management and/or trust services must be registered/licensed under the relevant legislation.

OBJECTIVE

These Guidelines give clarity on specific AMLCFT Obligations for TCSPs under Guyana's legislation, which includes requirements for robust Customer Due Diligence (CDD) and Enhanced Customer Due Diligence (EDD), proper record keeping measures, frameworks to fulfill statutory reporting obligations and monitoring and assessment of risks that are present in the use of legal structures and legal arrangements as well as in the operations of TCSPs themselves. These Guidelines also highlight other critical considerations that TCSPs should address to develop and maintain a dynamic framework that enables robust compliance measures to be effective.

MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING RISKS AND TRUST OR COMPANY SERVICE PROVIDERS

It is essential that TCSPs understand the importance of mitigating the risks of ML/TF/PF and other illicit activities. AMLCFT requirements for reporting entities operating in Guyana are primarily set out in the AMLCFT Act 2009 and AMLCFT Regulations 2023, Anti- Terrorism and Terrorist Related Activities Act, the Guyana Compliance Commission Act, inter alia.

All TCSPs registered in Guyana are required to have AML/CFT measures in place towards combatting global ML and TF. TCSPs are required to appoint a Compliance Officer. The duties of the Compliance Officer, include, inter alia, the development and implementation of the compliance framework, which addresses all areas of operation,.

The Compliance Framework must therefore be designed to prevent risks of a TCSP being used for ML.TF, PF and other risks. Awareness of the risks that exist with the formation and use of legal structures and legal arrangements is critical for TCSPs to develop a resilient compliance framework.

The Following Publications are relevant to TCSPs:

a. FATF Typologies study on the Misuse of Corporate Vehicles, including Trust and Company Service Providers[1]
b. FATF Report- Money Laundering Using Trust and Company Service Providers[2]
c. The Joint FATF and EGMONT Group Report on Concealment of Beneficial Ownership [3]
d. FATF Guidance for a Risk Based Approach for Trust and Company Service Providers[4]
e. FIU Guideline No. 2 of 2021 (Guyana)- Designated Non-Financial Businesses or Professions (DNFBPs) AMLCFT Compliance Regime[5]
f. FIU (Guyana) - AML/CFT Handbook for Reporting Entities[6]

[1] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Themisuseofcorporatevehiclesincludingtrustandcompanyserviceproviders.html
[2] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingusingtrustandcompanyserviceproviders.html
[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Egmont-Concealment-beneficial-ownership-Executive-summary.pdf
[4] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-trust-company-service-providers.html#:~:text=Risk%2Dbased%20Approach%20for%20Trust%20and%20Company%20Service%20Providers,-Filename%20RBA%2DTrust&text=These%20services%20include%3A%20acting%20as,an%20express%20trusts%2C%20among%20others. This Guidance is to be read in conjunction with the FATF Recommendations and in particular Recommendations 1, 10-12,17,19,20-25, and 28.

[5] https://fiu.gov.gy/wp-content/uploads/2022/12/DNFBP-AMLCFT-Compliance-Regime-Guideline-No-2-of-2021-PDF.pdf
[6] https://fiu.gov.gy/wp-content/uploads/2023/07/AMLCFT-Handbook-for-REs-Updated-June-30-2023.pdf

RISKS TO BE MONITORED BY TCSPs

TCSPs may be exposed to ML/TF/PF and other risks through their operations where criminals may seek to obscure the origin and ownership of criminally obtained assets through placement in legal structures or legal arrangements. Risks may also be presented where clients may seek services that are unusual or unconventional. Where TCSPs engage clients with exposure to jurisdictions that lack an effective framework for the supervision of AML/CFT Risks, a thorough risk assessment should be undertaken.

The FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers provides details that TCSPs should consider in carrying out risk identification and assessment.

Box 1 – Extract from the FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers

1. TCSPs should take appropriate steps to identify and assess the risk firm-wide, given the particular client base that could be used for ML/TF. They should document those assessments, keep these assessments up-to-date and have appropriate mechanisms in place to provide risk assessment information to competent authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

2. ML/TF risks can be organised into three categories: (a) country/geographic risk; (b) client risk, and (c) transaction/service and associated delivery channel risk. The risks and red flags listed in each category are not exhaustive but provide a starting point for TCSPs to use when designing their RBA.

3. TCSPs should also refer to their country's NRAs and risk assessments performed by competent authorities and supervisors.

4. When assessing risk, TCSPs should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supranational risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in TCSP services/sector, risk reports in other in other jurisdictions where the TCSP based in and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions.

5. TCSPs may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's

risk profiles are also important. Competent authorities should consider how they can best alert TCSPs to the findings of any national risk assessments, the supranational risk assessments and any other information which may be relevant to assess the risk level particular to a TCSP practice in the relevant country.

6. Due to the nature of services that a TCSP generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most TCSPs. The TCSP's knowledge of the client and its business will develop throughout the duration of a longer-term and interactive professional relationship. However, although individual TCSPs are not expected to investigate their client's affairs, they may be well-positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of the business relationship. TCSPs will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be, low risk (e.g. one-off client relationship). TCSPs should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

7. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow TCSPs to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the TCSP's role and involvement. Circumstances may vary considerably between TCSPs who represent clients on a single transaction and those involved in a long-term relationship.

8. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. A TCSP may also have to adjust the risk assessment of a particular client based on information received from a designated competent authority, SRB or other credible sources (including a referring TCSP.

9. TCSPs may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling TCSPs, where required, to subject each client to reasonable and proportionate risk assessment. 63. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the TCSP and/or firm. These criteria, however, should be considered holistically and not in isolation. TCSPs, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

Money Laundering and Terrorist Financing Risks in relation to 'shelf/shell companies'[7] being used by bad actors, also need to be considered. These include the obfuscation of key details such as the date of operations, origin of assets and beneficial ownership information. As such TCSPs must ensure that they are aware of the material risks presented by persons seeking 'shelf/shell companies'.

Furthermore, TCSPs must remain vigilant to emerging risks and new typologies that may diminish existing risk mitigation strategies. Therefore, TCSPs must be diligent in ensuring that their risk assessment frameworks are regularly updated and calibrated to changes in risks.

TCSPs must also ensure that their culture of compliance is not undermined by external factors, such as compliance provisions being imposed that do not appropriately address ML, TF, PF risks or risks of financial crime. These external factors may include inputs originating from an affiliate TCSP not licensed in Guyana or another entity that is associated with the subject TCSP through a Group of Companies.

[7] Shelf Company means an incorporated company with inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has already been established.

INSTITUTIONAL RISK ASSESSMENTS

TCSPs are required to assess the risk inherent in their own business, taking into consideration relevant factors, i.e. their customers, countries or geographical areas to which they are exposed, the products, services or transactions they offer and the delivery channels used to access customers. An institutional risk assessment should assist a TCSP in holistically understanding the ML/TF/PF risks to which it is exposed and identify the areas that should be prioritised to combat ML/TF/PF. For a TCSP, particular attention must be paid to the technology and cyber security risk it faces.

An important part of an institutional risk assessment is identification of the level of risks posed by each relevant factor and development of a risk rating. TCSPs must be able to identify the areas that pose higher risks and apply enhanced measures accordingly.

Records of the TCSP's institutional risk assessment must be maintained and made available to the **Guyana Compliance Commission** and all other competent authorities. Such records will include the findings, recommendations and steps taken to implement any recommendations. It is expected that the personnel at the highest level of a TCSP (i.e. directors/senior management) will consider and execute the findings of the institutional risk assessment.

RISK ASSESSMENT OF THIRD-PARTY INTRODUCTIONS

Section 15(8) of the AMLCFT Act as amended by Section 9 of AMLCFT Amendment Act No. 1 of 2015, provides that where a reporting entity relies on an intermediary or third party to undertake its obligations under **subsection (2), (3) or (4)** or to introduce business to it, it shall-

(a) Immediately obtain the information and documents required by subsections (2), (3), and (4);

(b) Take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to customer due diligence requirements will be made available from the third party upon request without delay;

(c) Satisfy itself that the third party or intermediary is regulated and supervised in accordance with international recommended best practices in relation to regulation and supervision, powers of supervisors and regulation and supervision of Designated Non-Financial Businesses and Professions and has measures in place to comply with customer due diligence requirements set out in international recommended best practices in relation to a terrorist financing offence and customer due diligence and record keeping, and in any event the ultimate responsibility for customer identification and verification shall remain with the reporting entity including where it seeks to rely on the third party.

A third party or introducer is an entity which introduces a customer to the reporting entity- a financial institution or a DNFBP that is supervised or monitored for, and has measures in place for compliance with CDD and Record Keeping requirements in line with FATF Recommendations 10 and 11.

A reporting entity is permitted to rely on a third party/introducer to undertake its CDD obligations in certain circumstances. If relying on a third party/introducer, the reporting entity must be satisfied that the third party/introducer —

(i) is regulated and supervised for AML/CFT purposes by a supervisory authority or by an equivalent regulatory or governmental authority, body or agency in Guyana or the jurisdiction in which he/she operates or in the case of a company, where it is registered or licensed to operate;

(ii) is subject to the AML/CFT Law or to equivalent legislation of another jurisdiction;

(iii) is licensed, registered, incorporated or otherwise established, whether in Guyana or a foreign jurisdiction that has an effective AML/CFT regime; and

(iv) is not subject to any secrecy or other law or circumstances that would prevent the reporting entity from obtaining any information or original documentation about the customer that the reporting entity may need for AML/CFT purposes.

When reliance is appropriate, after consideration of the above, the ultimate responsibility for CDD remains with the reporting entity - in other words, the reporting entity can delegate the task but not the responsibility. In such situations, the reporting entity should verify that the third party is conducting checks similar to or at a higher level than the reporting entity's own internal standards.

The reporting entity should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in FATF Recommendation 10, and also take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the relied upon institution upon request and without delay.

The Reporting entity must, in addition to the above, obtain the third party's full CDD Records which must include at a minimum the customer's –

- Name
- Address
- Date of Birth
- Principal business or Occupation
- Relationship with the third party

A risk assessment taken in relation to Introducers is required and should assist a TCSP to holistically understand the ML/TF/PF risks to which it or he or she is exposed and identify the areas that should be prioritised to combat ML/TF/PF. TCSPs should give particular attention to the risks based on the business activities/profession of the Third Party, as well as geographical and service risks that may be presented.

An important part of the risk assessment is to identify the level of risks posed by each relevant factor and develop a risk rating. TCSPs must be able to identify the areas that pose higher risks and apply enhanced measures accordingly. External factors can influence the frequency and/or risk rating of a Third Party. Therefore, TCSPs that rely on Third Parties may have to undertake more frequent risk assessments based on changing business activities, geopolitical factors or other circumstances that could impact a Third Party with whom they have a relationship.

Records of a TCSP's risk assessment of Third Parties must be maintained and made available to the FSC and all other competent authorities. Such records will include the findings, recommendations and steps taken to implement any recommendations. It is expected that the personnel at the highest level of a TCSP (i.e. directors/senior management) will consider and execute the findings of risk assessments conducted in relation to Third Parties.

Where a TCSP develops a suspicion of ML, TF or PF in relation to a Third Party, a suspicious activity report should be filed with the FIA. The TCSP should also take all appropriate steps to discontinue its relationship with the Third Party. Where a TCSP exits its relationship with a Third

Party, the TCSP must undertake thorough risk assessments of all related business prior to entering into direct business relationships with clients.

MATTERS FOR CONSIDERATION

(a) RECORD- KEEPING AND TRANSACTION MONITORING BY TCSPs

Section 16 of the AMLCFT Act 2009 as amended, requires TCSPs to maintain records that are sufficient to show and explain transactions and fiscal positions, as well as ensure that all customer due diligence records are obtained and maintained for at least seven (7) years from the date the relevant transaction was completed, or termination of business relationship, whichever is later.. TCSPs must also ensure that records are maintained in a manner that allows for retrieval without undue delay.

The reporting entity must keep records to provide sufficient information on the business relationship with the customer as follows:

- Records of the evidence of the customer's identity (eg. Copies or Records of official identification documents like passports, ID cards, driver's license.
- Records of account files and business correspondence in relation to transactions and identities of persons involved in the transactions (Eg. Inquiries to establish the background and purpose of complex, unusual large transactions)
- The name, date of birth, address and occupation of the customer, and where appropriate, the business or principal activity of each person conducting the transaction, on whose behalf the transaction is being conducted, as well as the method used by the reporting entity to verify the identity of each person;
- Records of the type and amount of currency involved in the transaction (e.g. the reporting entity must record, the type of currency - whether, United States dollar, Canadian dollar, Guyana dollar, etc., and also include, whether it is coin, paper money, bank notes or other negotiable instruments), including whether any other individuals or entities were involved in the transaction.
- Records of the nature and date of the transaction.

Maintenance of Records: A reporting entity must ensure that there is in place, an effective storage system that will facilitate the protection of documents. That is to prevent records from becoming, blurred, defaced, illegible, mutilated or in any other way deteriorated. Where records are being stored digitally or electronically, they must be easily retrievable or capable of reproduction in a printable and legible (readable) form.

Records Retrieval: Records must be retrieved promptly or without undue delay by the reporting entity. In other words, upon request for information by the FIU or other authorised authority, the reporting entity must ensure that the information is submitted (promptly) by the date specified by the requesting authority; or an order of the court.

Other record keeping functions: In addition to records of its customer's transactions, a reporting entity must also keep –
- a special register for AMLCFT enquires; and
- records of customer risk profiles.

The register of AMLCFT enquires must contain at a minimum:
- the date and nature of the enquiry;
- the name and agency of the inquiring officer;
- the powers being exercised and
- details of the accounts or transaction involved.

Records must be kept up to date and reviewed on an ongoing basis. Also, the reporting entity should establish safeguards for records, that is, a place for storage of back up, information offsite or onsite or other as may be determined by the reporting entity.

(b) CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) relates to the forestalling and preventing the activity of ML, TF and PF. TCSPs are considered to have business relationships with persons who seek services or products in the course of providing company management services and/or trust business services. In such circumstances Trust or Company Service Providers (TCSPs) must identify and verify the identity of customers pursuant to **Section 15 of the AMLCFT Act 2009** as amended.

The process of identifying and verifying the identity of a customer is commonly referred to a "customer due diligence" or "know your customer" (CDD / KYC). A reporting entity must carry out standard customer due diligence (CDD) for all its customers.

The CDD process should assist reporting entities to assess ML/TF risk associated with a business relationship. Reporting Entities should have policies, procedures, systems and controls which are up to date and effectively implemented to carry out CDD.

Standard CDD measures include:
• Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

• Identifying the beneficial owner and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the reporting entity is satisfied about the identity of beneficial owner.

• Understanding and obtaining information on the purpose and intended nature of the business relationship.

• Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the business and risk profile of the customer, including, where necessary, the source of wealth and source of funds
In addition, reporting entities should take measures to comply with national and international sanctions legislation; sanction screening is mandatory and is not discretionary.

As a general rule, reporting entities must apply CDD measures to all customers. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk associated with the individual business relationship. This means that the amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher or decreased where the associated risk is lower.

Reporting entities should conduct CDD on an initial and ongoing basis and should endeavour to be aware of material changes to the customer's legal form, beneficial ownership and nature of business.

A reporting entity should implement procedures to periodically review the customer relationship and CDD Information. The risk based periodic review process should be based on a formal cycle, and additional reviews should be performed based on "trigger event" causes.

In addition to carrying out CDD measures when one sets up a business relationship with a customer or carries out an occasional transaction, CDD should also be carried out if the TCSP:

- suspects ML, TF or PF;
- has determined that the relationship presents a higher-than-normal risk; or
- has any doubt about any information provided by the customer for identification or verification purposes.

To effectively carry out the act of CDD, a TCSP must:

- have systems to identify those persons who cannot produce standard documents;
- take account of the greater potential for money laundering in higher-risk cases, specifically in respect of politically exposed persons;
- not deal with persons or entities if due diligence cannot be executed or the results are not satisfactory; and
- have a system for keeping customer information up to date.

APPLYING CDD MEASURES

The extent to which CDD Measures are applied may vary to the extent that is permitted or required by law, based on the ML/TF/PF Risk identified or associated with the business relationship or a one-off transaction. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. Conversely, it may be simplified where the risk associated with the business relationship or transaction is lower. It should however be noted that applying and adopting simplified CDD measures is not acceptable where there is a suspicion of ML/TF/PF or where specific higher risk scenarios apply.

When designing CDD procedures and conducting CDD on customers, reporting entities should, where appropriate, consider the following issues:

• **Purpose and intended nature of business:** A reporting entity should ensure it has a clear understanding of expected activity to support ongoing transaction monitoring. Typically, the key consideration is being able to identify whether the customer's activity (e.g. transaction type, size or frequency) is in line with the reporting entity's knowledge of the customer. Understanding the nature of the business relationship includes understanding any other parties involved within the relationship. This includes verifying the authorisation of persons purporting to act on behalf of the customer, their identification and verification on a risk-sensitive basis and understanding the role the reporting entity plays. In higher risk situations, obtaining further information for ongoing monitoring of the business relationship and detection of potentially suspicious activity may be needed.

• **Beneficial ownership structures:** Where a customer appears to have a less transparent beneficial ownership or control structure, including the presence of corporate vehicles, nominees or private legal arrangements, a reporting entity should ensure to undertake reasonable steps to verify the identity of beneficial owner(s). Reporting entities should also consider whether the opacity of the ownership structure or the identity of one or more beneficial owners is an indicator of elevated risk and whether it is a cause or not for not performing the transaction or terminating the business relationship and considering making a suspicious transaction report.

• **Source of wealth and funds:** Under a Risk Based Approach, a reporting entity should take reasonable measures to establish the source of wealth and source of funds of relevant parties.

TCSPs are allowed to utilize technological mechanisms to effect CDD as well as record keeping, however, these measures must be consistent with the requirements to undertake CDD, primarily with respect to identifying and verifying applicants for business and customers, including beneficial owners.

Such technological developments must neither hinder the TCSPs' ability to effectively apply CDD measures nor the exchange of information with the FIU, supervisory authorities, or other competent authorities or law enforcement agencies.

SIMPLIFIED CDD MEASURES

Where a TCSP determines that a customer poses a significantly low risk, having regard to the ML, TF and PF risks identified by Guyana's national risk assessment, or a risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to ML, TF or PF in Guyana, simplified CDD measures may be applied.

In cases where a TCSP determines that simplified CDD measures may be applied, the following non-extensive actions may be taken:

- fewer elements of customer identification data may be obtained (production of one form of ID instead of two, for example);
- less robust identity verification procedures may be employed;
- collection of specific information, or the carrying out of specific measures to understand the purpose and intended nature of the business relationship may not be required (the purpose and nature of the business relationship may be inferred from the type of transactions or business relationship established);
- the identity of the customer and the beneficial owner(s) may be verified after the establishment of the business relationship.
- in the case of an existing business relationship, the frequency of customer identification updates may be reduced; and
- the degree and extent of ongoing monitoring and scrutiny of transactions may be reduced, based on a reasonable monetary threshold.d

ENHANCED DUE DILIGENCE (EDD)

EDD refers to the additional steps a TCSP is required to undertake to limit or manage the risk posed by a customer who poses a higher level of risk. This will be the case in relation, for instance, to a politically exposed person, a person from a jurisdiction that is considered to pose a high ML/TF risk, or a person who trades in products that are of a complex nature.

In cases where a TCSP determines that EDD measures should be applied, the following non-extensive actions may be taken:

- additional identifying information from a wider variety or more robust sources should be obtained and corroborated and the information used to inform the individual customer's risk profile;
- additional searches (e.g. verifiable adverse internet searches) should be carried out to better inform the individual customer's risk profile;
- where appropriate, further verification procedures should be undertaken on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may pose to the TCSP;
- the source of funds and wealth involved in the transaction or business relationship should be verified to satisfy the TCSP that they do not constitute the proceeds of crime;
- the information provided with regard to the destination of funds and the reasons for the transaction should be evaluated; and
- additional information about the purpose and intended nature of the transaction or the business relationship should be sought and verified.

TCSPs should also consider the following specific higher-risk factors, which may also trigger the need to conduct EDD:

a) Clients are connected to industries or sectors where opportunities for ML and TF are particularly prevalent. These may include clients that:

- become a politically exposed person; and
- operate or reside in a jurisdiction that is subject to recent sanctions or has been recently listed as having major deficiencies in their AML/CFT framework.

b) The client:

- is involved in the shipment and/or sale of dual-purpose goods;
- has been transferred to a TCSP's portfolio with little or no notification;
- changes or expands its business activities into volatile markets;
- frequently requests endorsements from the TCSP on their bona fides; and
- refuses to send complete information following a request made for more clarification for a transaction or other activity.

8.5.3. Where a TCSP is unable to verify the identity of an individual after carrying out EDD, it should not enter a business relationship or execute a one-off transaction with that individual. If the business relationship already exists, the TCSP should terminate the business relationship.

In all circumstances, the TCSP should consider filing a suspicious transaction report with the FIU in relation to the customer or individual.

ONGOING CDD AND TRANSACTION MONITORING

Once a business relationship is established, TCSPs have an obligation to ensure that CDD/EDD measures are carried out on an ongoing basis. Such measures are required to determine whether executed transactions are consistent with the TCSP's information about the customer and the nature and purpose of the business relationship, wherever appropriate.

These ongoing CDD/EDD measures should allow TCSPs to identify changes in customer profiles (for example, their behaviour, use of products and the amount of money involved), and to keep them up to date, which may require the application of enhanced CDD measures.

An essential component in identifying transactions that are potentially suspicious is transaction monitoring. Transactions that do not fit the behaviour expected from a customer's profile or that deviate from the usual pattern of transactions may be potentially suspicious. Where new patterns of transactions emerge, TCSPs should ensure that measures are taken to determine whether there is an increased risk of ML, TF or PF. TCSPs must also consider non-cash transactions in their monitoring processes; for example, a non-cash transaction includes requests for the provision of corporate documents. Changes in the pattern of such requests should also be factored into the assessment of ML/TF/PF risks. Monitoring should, therefore, be carried out on an ongoing basis.

The level of transaction monitoring should be based on a TCSP's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher-risk situations. The adequacy of a TCSP's monitoring system, and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the TCSP's AML/CFT/CPF risk programme.

Transaction monitoring systems may be manual or automated based on the volume of transactions processed by a TCSP on a regular basis. However, where automated systems are used, TCSPs should understand their system tolerances, verify their suitability and integrity on a regular basis and verify that they take account of identified ML/TF/PF risks.

Transactions performed or initiated by an outsourced party must also be subject to regular monitoring under the same conditions as transactions of the TCSP itself. Such monitoring should

be conducted under the TCSP's control by the TCSP itself, or in collaboration with a third party, based on appropriate agreements complying with requirements of the AMLCFT Act 2009, as amended.

TCSPs should consider creating thresholds in relation to clients' assets under management, based on a risk-based approach, to determine the level of scrutiny for transaction monitoring purposes. Additionally, TCSPs should properly document, retain and communicate to the relevant personnel, including senior management and front-line staff, the results of their monitoring, as well as any queries raised and resolved. TCSPs must also undertake relevant training with regard to transaction monitoring.

TARGETED FINANCIAL SANCTIONS AND SANCTION SCREENING

The AML/CFT legislation establishes a legal framework for asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of a listed person or entity.

A listed person or entity is:

(i) Any person or entity designated pursuant to **United Nations Security Council Resolution (UNSCR) 1267/1999** and its successor resolutions;
(ii) Any person or entity specified by Guyana pursuant to **UNSCR 1373(2001)** and its successor resolutions;
(iii) Any person or entity designated by the **1718 Sanctions Committee of the Security Council** in accordance with **UNSCR 1718 (2006)** and its successor resolutions; or
(iv) Any person or entity designated by the **2231 Sanctions Committee** in accordance with **UNSCR 2231(2015)** and its successor resolutions.

Once it is established that a customer is a listed person or entity, the reporting entity must immediately inform the Director-FIU.

For further information see:

1) Guide on Implementing Targeted Financial Sanctions Measures Guideline No. 2 of 2015 issued by the FIU
2) Targeted Financial Sanctions related to Terrorism and Terrorism Financing Guideline No. 3 of 2015 issued by the FIU
3) Targeted Financial Sanctions related to Terrorism, Terrorism Financing and Proliferation Financing Guideline No. 1 of 2022 issued by the FIU.

It is expected that TCSPs should be able to screen their client base immediately upon receiving a designation notice in order to identify any designated persons and take appropriate measures in keeping with the requirements of the relevant sanctions Orders, including asset freezing and compliance reporting. TCSPs must also ensure that they have mechanisms in place to promptly act on new designations.

FILING OF SUSPICIOUS ACTIVITY/TRANSACTION REPORTS

TCSPs must ensure that their compliance frameworks include mechanisms, policies, procedures, and internal controls to promptly report suspicious transactions/activities internally and report suspicious transactions and activities to the FIU. TCSPs must ensure that any mechanism accounts for, amongst other things, attempted activity and transactions or customer relationships that the TCSP has refused.

Accordingly, TCSPs are required to appoint a qualified individual as the Compliance Officer to file Suspicious Transaction Reports pursuant to Section 15 of the AML/CFT Act 2009.

Some RED Flags or patterns of behaviour include the following and should be read in conjunction with any other document issued by the FIU, other relevant competent authority or FATF:

- clients conducting business through or requesting services that involve unusual or complex structures without a rationale that is clear and understandable to the TCSP;
- unexplained urgency in requesting services or products;
- requests from clients that do not provide a clear explanation to the TCSP;
- frequent or irregular changes of beneficial ownership or controllers or other fiduciaries of a legal structure or legal arrangement;
- unexpected and/or frequent changes in the business activities of a legal structure or legal arrangement;
- transactions that have no apparent benefit or purpose to the client or involves a closely connected person or entity with whom the TCSP has no business relationship with;
- changes in method of payment for services at the last minute and without justification, or a transaction is being completed through a third party (this excludes a client that is linked to a third party that the TCSP relies upon in line with FATF Recommendation 17);
- use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason; and
- clients that start or develop an enterprise with an unexpected profile or abnormal business cycles or clients that enter into new/emerging markets.

There may be other emerging practices that are indicative of suspicious patterns or behaviour. As such, TCSPs are to remain vigilant and review publications of typologies of risks in relation to the use of legal structures and legal arrangements. The FATF Guidance on Transparency and Beneficial Ownership should be considered by TCSPs in the development of their risk assessment frameworks. TCSPs should also consider the FATF Guidance for a Risk-Based Approach for the Accounting Profession, as well as the FATF Guidance for a Risk-Based Approach for Legal Professionals where their activities extend to the accounting and legal services sectors. TCSPs

should also pay particular attention to their specific circumstances and customers to ensure that they are able to identify suspicious factors which may present themselves or be unique to the TCSP, its services, products, or its client base.

TCSPs should also be mindful that if it, or an employee, knows or suspects that an ML/TF/PF investigation is happening or about to take place, it is an offence to disclose information to anyone else, which is likely to prejudice that investigation. Equally, if the TCSP knows or suspects that a disclosure of suspicion has been or is being made, it is an offence to leak information that could prejudice any investigation conducted. This extends beyond ML, TF, PF or other investigations to disclosures which would prejudice a confiscation investigation. Interfering with documents and other materials relevant to an investigation is also an offence. TCSPs must therefore ensure that all staff are appropriately trained and understand their legal obligations in relation to tipping off.

OTHER RISK INDICATORS- CONCEALEMENT OF BENEFICIAL OWNERSHIP

The FATF and Egmont Group of Financial Intelligence Units carried out a study that examined mechanisms and techniques that can be used to obscure the ownership and control of illicitly gained assets. The resultant report from this joint study – Concealment of Beneficial Ownership was published in 2018 and focused on services provided by lawyers, accountants and TCSPs. Three areas that are of particular relevance for TCSPs in the development of their ML and TF risk mitigation strategies have been covered below.

(a) Generating complex ownership and control structures

Bad actors may use complex chains of ownership to disguise beneficial ownership by using numerous layers of legal structures and legal arrangements. These legal structures and legal arrangements may be incorporated or otherwise established in multiple jurisdictions and may also be formed through the use of different DNFBPs (such as lawyers, accountants or other foreign TCSPs). While complexity in and of itself is not illegal, TCSPs should undertake additional steps to ensure that they are not being used to obscure beneficial ownership that could further ML, TF, PF or other financial crimes.

In assessing complex structures, TCSPs should ensure that they assess whether features that present heightened risks are present. These may include:

— Shell companies (that is, companies with no real economic activity);
— Straw men (persons who are included in the ownership structure to conceal the true beneficial ownership of a legal structure); and
— Illegal phoenix activity (where a company is created to continue the operations of another company to avoid paying creditors, taxes, and other liabilities).

(b) Obscuring of a relationship between beneficial owners and assets

As such, bad actors may seek to use nominee shareholders and directors to disguise beneficial ownership and/or control of a legal structure or legal arrangement. Bad actors may also use informal nominee shareholders and directors who are typically personal connections of the true beneficial owner for the purpose of maintaining a fiction of ownership. This practice is often cited as the use of "front" men or "straw" men. These persons acting as "front" men may be unaware of the true activities of the legal structure that they act for. Bad actors may also use stolen identities to establish legal structures. For example, the victims of identity theft may be used as nominees, shareholders or directors without their consent. Given the risks that may be present in the use of nominee shareholders or in the provision of directorship services, TCSPs must ensure their risk assessment processes are sufficiently robust to detect and mitigate against these risks.

(c) Falsifying activities

Bad actors may hide beneficial ownership through criminal activities, which include the falsification of documents. Several methods have been identified that have been used for this purpose. More common schemes include:

— False loans and invoices, and other transactional documents to disguise the beneficial ownership of a transaction (or multiple transactions).
— Use of “load-back” schemes where a loan is issued to a third party following the payment of a business invoice.
— Falsifying prospectuses, accounting records and other statements to attain a favourable outcome in a registration, acquisition, or other business transaction.

TCSPs are guided to ensure that they keep abreast of future developments and publications by the FATF and other international standard setters in relation to developing risk indicators.

(d) Bearer Shares

Pursuant to Section 28 of the Companies Act of Guyana, no Company shall issue bearer shares or bearer share certificates.

The use of bearer shares and similar instruments continues in other jurisdictions. Therefore, TCSPs must be vigilant where foreign legal structures may be utilised by a customer or applicant for business and may contain bearer shares, bearer warrants or other similar instruments. In such cases, TCSPs must ensure that they conduct enhanced due diligence and determine whether there is a valid reason for the use of such instruments. Due to the nature of bearer shares, TCSPs must ensure that they can effectively monitor beneficial ownership on an ongoing basis or exit a business relationship where beneficial ownership cannot be accurately determined and monitored, including due to bearer shares.

(e) Employee Screenings

TCSPs must ensure that they screen their employees in accordance with section 19 of the AMLCFT Act 2009, as amended. To safeguard against ML, TF, PF and other risks, measures must be in place to assess the competence and probity of employees at the time of recruitment and intermittently thereafter. These assessments of employees must include background checks as well as an assessment of integrity, skills, knowledge, and expertise to ably carry out their functions. Additional assessments and screening of employees must also be carried out to mitigate against operational and compliance risks where there is an anticipated change in their role or functions. This is of particular importance where the employee is responsible for the implementation of or monitoring of AML/CFT/CPF controls, which may occur directly in relation to the compliance function or indirectly in relation to other functions.

TCSPs must also ensure that the screening of employees is proportionate to the ML/TF/PF risks to which that employee may be exposed, regardless of the level of seniority of any employee. In addition, systems must be established to address potential conflicts of interest for staff with AML/CFT/CPF responsibilities. TCSPs must also be aware of their responsibility to report employee misconduct to the FIU and, where relevant, any other competent authority or law enforcement agency.

POWER OF THE GUYANA COMPLIANCE COMMISSION

The Guyana Compliance Commission is the supervisory authority appointed to supervise Trust and Company Service Providers in Guyana pursuant **to Section 4 of the Guyana Compliance Commission Act 2023** which provides:

" 4.(1) The Commission shall function as a supervisory authority as designated under the Anti-Money Laundering/Countering the Financing of Terrorism Act.

(2) The powers and functions of the Commission are —

(a) to maintain a general review of designated non-financial businesses or professions, non-profit organisations and non-bank financial institutions-

(i) in relation to the conduct of financial transactions; and

(ii) to ensure compliance with the provisions of the Anti-Money Laundering and Countering the Financing of Terrorism Act;

(b) to conduct on-site and offsite examinations of the business of a reporting entity when deemed necessary by the Commission at the expense of the reporting entity, for the purpose of ensuring compliance with the provisions of this Act and the Anti-Money Laundering and Countering the Financing of Terrorism Act , and in such cases where the Commission is unable to conduct such examination, to appoint an auditor at the expense of the reporting entity, to conduct such examination and to report to the Commission;

(c) to ensure that its reporting entities-

(i) implement and update their anti-money laundering and countering the financing of terrorism policies and

(ii) that the policies are based on the anti-money laundering and countering the financing of terrorism legislation and best practice standards;

(d) to give effect to all supervisory functions and to monitor and ensure compliance by reporting entities of their obligations under section 15,

16,18,19,20 sections 68A, 68B, 68C, 68D, 68F, 68G, 68H and 68I, sections 75A and 75B, and all other reporting entity obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Act and regulations made thereunder;

(e) collect, store, and disseminating, to interested parties, reliable and timely information on the growth and trends related to its reporting entities;

(f) in relation to its reporting entities, monitor and enforce all requirements under sections 22 and 23 of the Anti-Money Laundering/Countering the Financing of Terrorism Act and its regulations made thereunder;

(g) where specified by the Minister by order, issue licences, registration, permits or authorisations including terms, conditions and limitations;

(h) at the request of a domestic regulatory authority, exercise its powers under this Act to assist with the performance by the domestic regulatory authority of its functions;

(i) examine and investigate the affairs of a reporting entity in accordance with this Act;

(j) undertake any review necessary to ensure compliance with the Act; and

(k) any other function as the Minister may specify by order.

(3) For the purposes of discharging its functions, the Commission may establish ad-hoc or permanent committees to foster coordination among public entities or between public and private entities or for the purposes of collaboration and cooperation, as necessary, on anti-money laundering/countering the financing of terrorism/countering proliferation financing matters.

INFORMATION EXCHANGE

Where authorities are armed with suspicion or evidence of a person's link or suspected link to ML, TF, or PF, they should be able to share that information with the TCSPs so that the latter can better engage its processes in dealing with such a person. Conversely, TCSPs should also be able to share general information about the type and nature of suspicious activities that may be linked to ML, TF or PF with other financial institutions and government agencies, including the regulator, subject to the requirements to ensure that there is no tipping off related to the filing of a SAR. This can only help to strengthen the TCSP sector and insulate it from abuse and misuse for ML, TF and PF purposes.

There are various types of information that can be shared between regulatory and law enforcement agencies and TCSPs. Such information may include:

- ML/TF/PF risk assessments;
- General feedback on suspicious transaction reports and other relevant reports;
- Typologies of how money launderers or terrorist financiers have misused TCSPs;
- Targeted unclassified intelligence which, subject to appropriate safeguards such as confidentiality agreements, may be shared with TCSPs, either collectively or individually; and
- Sanctions lists

Domestic cooperation and information exchange between TCSPs, the FIU and the Guyana Compliance Commissioner (as the supervisor of the TCSP sector), among law enforcement and intelligence agencies, is extremely important in the effective monitoring and/or supervision of the TCSP sector.

Cross-border information sharing between authorities and their international counterparts with regard to information held within the TCSP sector is also vitally important given the multi-jurisdictional reach of many TCSPs. TCSPs must ensure that they fully comply with the CDD and record-keeping requirements, as well as all other requirements of the AMLCFT Act 2009 and AMLCFT Regulations, to ensure that Guyana is able to meet its international cooperation obligations, including those relating to beneficial ownership.

OVERARCHING REQUIREMENTS FOR COMPLIANCE

All TCSPs must remain vigilant in relation to evolving ML, TF and PF threats, as well as other threats that can negatively impact their operations. To mitigate these threats and risks, TCSPs must be diligent in the application of AML/CFT/PF measures. These measures must be holistic and integrate prudent governance and modern risk management strategies with a robust compliance framework. TCSPs must remain agile and embed systems to allow for continual improvement in the efficiency and effectiveness of compliance.

APPENDIX 1

RED FLAGS

There are a myriad of ways in which money laundering or terrorism financing may occur. Below is a non–exhaustive list of "Red Flags" that may warrant closer attention.

Financial institutions are encouraged to refer to such organizations as the FATF, Egmont Group and United Nations Office on Drugs and Crime for typology reports and sanitised cases on money laundering and terrorist financing schemes, respectively.

IF THE CLIENT:

- Does not want correspondence sent to home address
- Shows uncommon curiosity about internal systems, controls and policies
- Over justifies or explains the transaction
- Is involved in activity out-of-keeping for that individual or business

IF THE CLIENT:

- Produces seemingly false identification or identification or identification or information to be counterfeited, altered or inaccurate
- **Provides insufficient, false or suspicious information, or information that is difficult or expensive to verify**

ECONOMIC PURPOSE

- Transaction is unnecessarily complex for its stated purpose
- Activity is inconsistent with what would be expected from declared business
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Accounts that show virtually no banking activity but are used to receive or pay significant amounts not clearly related to the customer or the customer's business.

CASH TRANSACTIONS

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past
- Frequent exchanges small bills for large ones
- Deposits of small amounts of cash on different successive occasions, in such a way that on each occasion the amount is not significant, but combines to total a very large amount (ie. Smurfing)
- Consistently making cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.

— Stated occupation is not in keeping with the level or type of activity (eg. Student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over wide geographic area)
— Unusually large deposits or withdrawals of cash by an individual or legal entity whose apparent business activities are normally carried out using cheques and other monetary instruments.
— Multiple and frequent purchase or sale of foreign currency by a tourist
— Multiple and frequent large withdrawals from an ATM using a local debit card issued by another financial institution
— Multiple and frequent large withdrawals from an ATM using debit or credit card issued by a foreign financial institution

DEPOSIT ACTIVITY

— Account with a large number of small cash deposits and a small number of large cash withdrawals
— Funds are being deposited into several accounts, consolidated into one and transferred outside the country
— Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers
— Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
— Account that was reactivated from inactive or dormant status suddenly exhibits significant activity
— Reactivated dormant account containing minimal sum suddenly receives a deposit or series of deposits are made to a client's account by third parties.
— Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.

CROSS BORDER TRANSACTIONS

— Deposits followed within a short time by wire transfers to or through locations of concern such as countries known or suspected to facilitate money laundering activities.
— Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system
— Immediate conversions of funds transfers into monetary instruments in the name of third parties.
— Frequent sending and receiving of wire transfers, especially to or from countries considered high risk for money laundering or terrorist financing, or with strict secrecy laws. Added attention should be paid if such operations occur through small or family run banks, shell banks or unknown banks.
— Large incoming or outgoing transfers with instructions for payment in cash

— Client makes frequent or large electronic funds transfers for person who have no account relationship with the institution.
— Client instructs you to transfer funds abroad and to expect an equal incoming transfer
— Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country
— Wire transfers are received from entities having no apparent business connection with client.

PERSONAL TRANSACTIONS

— Client has no employment history but make frequent large transactions or maintains a large account balance
— Client has numerous accounts and deposits cash into each of them with the total credits being a large amount
— Client frequently makes automatic banking machine deposits just below the reporting threshold.
— Increased use of safety deposit boxes. Increased activity by the person holding the boxes. The Depositing and withdrawal of sealed packages.
— Third parties make cash payments or deposit cheques to a client's credit card
— Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

CORPORATE AND BUSINESS TRANSACTIONS

— Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which is inconsistent with the client's business.
— Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity
— Unexplained transactions are repeated between personal and business accounts.
— A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

LENDING

— Customer suddenly repays a problem loan unexpectedly, without indication of the origin of the funds
— Loans guaranteed by third parities with no apparent relation to the customer

— Loans backed by assets, for which the source is unknown or the value has no relation to the situation of the customer.
— Default on credit used for legal trading activities, or transfer of such credits to another company, entity or person, without any apparent justification, leaving the bank to enforce the guarantee backing the credit.
— Use of standby letters of credit to guarantee loans granted by foreign financial institutions, without any apparent economic justification.

SECURITIES

— Client frequently makes large investments in stocks, bonds, investments trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
— Client makes large or unusual settlements of securities in cash.
— Client is willing to deposit or invest at rates that are not advantageous or competitive.

ACCOUNTS UNDER INVESTIGATION

— Accounts that are the source or receiver of significant funds related to an account or person under investigation or the subject of legal proceedings in a court or other competent national or foreign authority in connection with fraud, terrorist financing or money laundering.
— Accounts controlled by the signatory of another account that is under investigation or the subject of legal proceedings by a court or other competent national or foreign authority with fraud, terrorist financing or money laundering.

FIDUCIARY BUSINESS

— Client seeks to invest a large sum of money with no apparent interest in the details of the product and does not enquire about the characteristics of the product and or feigns market ignorance
— Corporate client opens account with large sum of money that is not in keeping with the operations of the company, which may itself have recently been formed.
— Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.

EMPLOYEES

— Lifestyle, financial status or investment activity is not in keeping with the employee's known income
— Reluctance to go on vacation, to change job position or to accept a promotion, with no clear and reasonable explanation.

- Employee frequently receives gifts/and or invitations from certain clients, with no clear or reasonable justification
- Employee hinders colleagues from dealing with specific client(s) with no apparent justification
- Employee documents or partially supports the information or transactions of a particular client with no clear and reasonable justification
- Employee frequently negotiates exceptions for a particular client(s).

TERRORIST FINANCING INDICATORS

The Egmont Group reviewed 22 terrorist financing cases submitted by financial intelligence units (FIUs) and compiled financial and behavioral indicators that were most frequently observed indicators associated to terrorist financing. Behaviour indicators include:

- The parties to the transaction (owner, beneficiary, etc.) being from countries known to support terrorist activities and organizations
- Use of false corporations, including shell companies
- Inclusion of the individual in the United Nations 1267 Sanctions list
- Media reports that the account holder is linked to known terrorist organization or is engaged in terrorist activities
- Beneficial owner of the account is not properly identified
- Use of nominees, trusts, family member or third-party accounts
- Use of false identification
- Abuse of nonprofit organizations Indicators linked to financial transactions
- The use of funds by nonprofit organization is not consistent with the purpose for which it was established
- The transaction is not economically justified considering the account holder's business or profession
- A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds
- Transactions that are inconsistent with the account's normal activity
- Deposits were structured below the reporting requirements to avoid detection
- Multiple cash deposits and withdrawals with suspicious references
- Frequent domestic and international ATM activity
- No business rationale or economic justifications for the transactions
- Unusual cash activity in foreign bank accounts
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country
- Use of multiple foreign bank accounts

PROLIFERATION FINANCING INDICATORS

- When customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to higher risk jurisdictions.
- When 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.
- The customer is a research body connected with a higher risk jurisdiction of proliferation concern.
- When customer's activities do not match with the business profile provided to the reporting entity.
- When customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.
- When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.
- When a freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.
- When final destination of goods to be imported / exported is unclear from the trade related documents provided to the reporting entity.
- Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.
- The transaction(s) involve an individual or entity in any country of proliferation concern.
- The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.
- The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.
- Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.
- When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason.

APPENDIX 2

VERIFICATION EXAMPLES

A. Personal Clients

- Confirm the date of birth from an official document (e.g. birth certificate).
- Confirm the permanent address (e.g. utility bill, tax assessment, bank statement, letter from a public notary).
- Contact the customer e.g. by telephone, letter, email to confirm information supplied
- Confirming the validity of the official documents provided through certification by an authorised person.
- Confirm the permanent and/ business residence through credit agencies, home visits
- Obtain personal references from third parties and existing customers in writing.
- Contact issuers of references.
- Confirmation of employment.

B. Corporate Customers & Partnerships

- Review of current audited information (preferably audited).
- Obtain statements of affairs, bank statements, confirmation of net worth from reputable financial advisers.
- Seek confirmation from a reputable service provider(s).
- Confirm that the company is in good standing.
- Undertake enquiries using public and private databases.
- Obtain prior banking and commercial references, in writing.
- Contact issuers of references.
- Onsite visitations.
- Contact the customer e.g. by telephone, letter, email to confirm information supplied.

C. **Trusts and Fiduciary Clients**

- Seek confirmation from a reputable service provider(s).
- Obtain prior bank references.
- Access public or private databases.

APPENDIX 3

CONFIRMATION OF CUSTOMER VERIFICATION OF IDENTITY

Part A - Personal Customers

Full Name of Customer: (Mr/Mrs/Ms)
…….
Known Aliases:……..……
Identification:…….…...
Current Permanent Address:…….
Date of Birth:……. Nationality:…….....
Country of Residence:……
Specimen Customer Signature Attached: **Yes ___ No__**

Part B - Corporate & Other Customers

Full Name of Customer:……
Type of Entity: ……..
Location & domicile of Business: ……
Country of Incorporation: …….
Regulator / Registrar: ……
Names of Directors: ……..
……
Names of majority beneficial owners:……...
……

Part C

We confirm that the customer is known to us. **Yes ___No ____**

We confirm that the identity information is held by us. **Yes___ No ___**

We confirm that the verification of the information meets - the requirements of Guyana law and AML/CFT/CPF Guideline. **Yes ___ No __**

We confirm that the applicant is acting on his own behalf and - not as a nominee, trustee or in a fiduciary capacity for any - other person. **Yes ____No ___N/A _____**

Part D

Customer Group Name: ……

Relation with Customer: ……...

Part E

Name & Position of Preparing Officer: ……

(*Block Letters*)

Signature & Date:……..

Name & Position of Authorising Officer:……..

(*Block Letters*)

Signature & Date:……..…….