TURKS AND CAICOS ISLANDS

FINANCIAL SERVICES COMMISSION

Regulating with Honesty, Integrity and Transparency

DNFBP GUIDANCE ON DUE DILIGENCE AND ENHANCED DUE DILIGENCE FOR HIGH-RISK CUSTOMERS – APPLYING A RISK BASED APPROACH

19 March 2021

DEFINITIONS

AML/CFT	AML means Anti-Money Laundering and CFT means Counter Financing of Terrorism.
Anti-Money Laundering and Prevention of Terrorist Financing Legislation ("AML Legislation")	▪ Proceeds of Crime Ordinance Cap.03.15 (POCO) ▪ Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010 ▪ Anti-Money Laundering and Prevention of Terrorist Financing Code 2011 ▪ Prevention of Terrorism Ordinance, Cap 3.21 ▪ Companies Ordinance 2017 ▪ Financial Intelligence Agency Ordinance Cap. 3.20 ▪ Financial Services Commission Ordinance Cap.16.01 ▪ Terrorist Asset-Freezing, etc. Act 2010 (Overseas Territories) Order 2011 ▪ Sanctions Orders extended to the TCI by the United Kingdom
Designated Non-Financial Businesses and Professions (DNFBP)	A financial business, as set out under Schedule 2 of the Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010 (AML Regulations), that is not a regulated financial business as set out under Schedule 1 of the AML Regulations.
FATF	The Financial Action Task Force (FATF) is an inter-governmental organization that designs and promotes policies and standards to combat financial crime. Recommendations created by FATF target money laundering, terrorist financing, and other threats to the global financial system. FATF was created in 1989 at the behest of the G7 and is head-quartered in Paris.
FATF 40 Recommendations	FATF has issued 40 recommendations representing a complete set of countermeasures against money laundering (ML) covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation. These recommendations have been recognised, endorsed, or adopted by many international bodies.
Financial Intelligence Agency (FIA)	The FIA plays a central role in the TCI's AML/CFT regime and serves as the national centralised agency that is responsible for the receipt, analysis, and dissemination of SARs from financial institutions (FIs) and DNFBPs.
High value dealers	A business: (a) dealing in vehicles (b) pawning or (c) trading in goods, precious metals, or precious stones, when it receives, in respect of any transaction whether the transaction is executed in a single operation or in several linked operations, a payment or payments in cash or other form of at least $15,000 or the equivalent in another currency.
Legal entity	Legal person such as a company, or legal arrangement such as a partnership or trust.

Money Laundering (ML)	Money laundering is the processing of criminal proceeds to disguise their illegal origin.
Natural person	Refers to an individual.
Ongoing monitoring	Ongoing monitoring means: (a) Scrutinising transactions undertaken throughout the course of the relationship including, where necessary, the source of funds to ensure that the transactions are consistent with the financial business' knowledge of the customer, his business, and his ML/TF risk profile. (b) Keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date and relevant by undertaking reviews of existing records.
Politically Exposed Person (PEP)	A PEP is a) an individual who is or was entrusted with prominent public functions by the TCI, by a foreign State, or by an international body or organization; b) an immediate family member of a person referred to a) immediately above; or c) a known close associate of a person referred to in a) immediately above. DNFBPs should have appropriate risk management systems to determine if a customer, a person in control of the customer, or the beneficial owner of a customer, is a PEP.
Risk-sensitive/Risk Based Approach (RBA)	An RBA is a procedure or process for DNFBPs to identify, assess and understand the ML/TF risks to which they may be exposed, and take relevant and adequate AML/CFT measures, commensurate to those risks, to mitigate them effectively. When assessing ML/TF risk, countries, competent authorities and DNFBPs should analyse and seek to understand how the ML/TF risks they identify, affect them. Thus, the risk assessment process provides the basis for the risk-sensitive application of AML/CFT measures.
Source of Funds	The "source of funds" is the business, transaction or other activity that generates the funds for a customer, which may include the customer's occupation.
Source of Wealth	A person's "source of wealth" means the business, transactions or other activities that have generated the total net worth of a person. It should be noted that it is the source of the person's wealth that is important rather than the amount of it. It may not, therefore, be necessary for information on the amount of wealth to be obtained.

Suitable certifier	The AML Code requires that a certifier be subject to professional rules (or equivalent) which provide the financial business with a reasonable level of comfort as to the integrity of the certifier. A suitable certifier may include: (a) any person approved by the Commission (b) a member of the judiciary (c) a senior public servant (d) a serving police or customs officer (e) an officer of an embassy, consulate, or high commission of the country issuing the documentary evidence of identity (f) a lawyer who is a member of a recognised professional body (g) a notary public who is a member of a recognised professional body (h) a notary public equivalent (an officer who by their employment or commission is recognised by the TCI government to take and administer oaths) (i) an actuary who is a member of a recognised professional body (j) an accountant who is a member of a recognised professional body (k) a director, officer, or manager of a regulated person based in the TCI (l) a director, officer, or manager of a branch or subsidiary of a group, head-quartered in a well-regulated jurisdiction, which applies group standards to subsidiaries and branches worldwide, and which tests the application and compliance with such standards.
Suspicious Activity Report (SAR)	A Suspicious Activity Report (SAR) is a document that the MLRO of the DNFBP is required to file with the Financial Intelligence Agency (FIA) whenever there is a suspected case of money laundering or terrorist financing.
Terrorist Financing (TF)	Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.

AUTHORITY

1. This guidance is issued by the Turks and Caicos Islands Financial Services Commission (the "Commission") as the supervisor of Designated Non-Financial Businesses and Professions (DNFBPs), pursuant to Regulation 23 of the Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010 (the "AML Regulations"). The Commission is vested with responsibility for determining compliance by DNFBPs with the AML Regulations, the Anti-Money Laundering and Prevention of Terrorist Financing Code 2011 (the "AML Code"), and the Anti-Money Laundering and Prevention of Terrorist Financing Guidance Notes (the "AML Guidance Notes").

PURPOSE

2. This guidance is designed to assist DNFBPs in complying with Regulation 11 of the AML Regulations, and Part 3 of the AML Code, both of which concern customer/client due diligence (CDD) measures to enable DNFBPs to implement an effective compliance regime that would enable them to detect, identify, and mitigate their money laundering or terrorist financing risks.

3. The information provided represents broad measures and must be used in conjunction with the AML Regulations, AML Code and AML Guidance Notes. This guidance is not a "one size fits all" as the DNFBP sector is made up of several sub-sectors for which the application of some of the CDD measures outlined may be impractical. This is particularly true for the high value dealers sector, where the application of CDD measures extends only to customers purchasing goods, precious metals, or precious stones, in the amount of USD $15,000 and above, or the equivalent in another currency, whether the goods are purchased in a single transaction or in several instalments which are linked.

4. All DNFBPs are required to apply a risk-based approach (RBA), based on the assessment of risks associated with the DNFBP, commensurate with the DNFBP's size, nature, and complexity. All DNFBPs must be able to demonstrate the effectiveness of their AML compliance program to prevent, detect and mitigate any risk of money laundering or terrorist financing.

SCOPE

5. This guidance applies to DNFBPs which include the following categories of business as listed in Schedule 2 of the AML Regulations:
   - Independent legal professions
   - Accountancy or auditing services
   - Real estate agents
   - High value dealers

- Lenders and/or lending agents
- Payment service providers

High Value Dealers (HVD)

6. TCI law defines a business as a HVD where it deals in vehicles, pawning, or trades in precious metals or precious stones, or trades in goods or services of any description, when it receives payment in cash or credit card of at least $15,000 or the equivalent in another currency. This applies whether the transaction is executed as a single transaction or in several instalments which are linked. Businesses that only occasionally accept or make such transactions are included in the definition and are subject to the AML legislation. Businesses that do not meet the high value payment threshold are not affected.

7. Generally, the businesses most affected will be those that deal in high value or luxury goods, works of art, cars, jewellery, and yachts. However, the regime applies to everyone who accepts sufficiently large amounts of cash for goods and any business could potentially be registrable.

8. If a HVD does not intend to accept high value payments it should have a written policy to this effect and ensure that employees and customers are aware of this policy.

STATUS OF THIS GUIDANCE

9. This guidance is supplemental to the AML Regulations and AML Code. It is not legal advice and is not intended to replace the AML Regulations and the AML Code. The guidance is intended for use by senior management and compliance staff of DNFBPs to assist in the development of internal systems and controls. However, compliance with this guidance will be taken into consideration by the Commission when assessing a DNFBP's compliance with their legal obligations.

SPECIFIC CDD REQUIREMENTS RELATING TO DNFBPs

10. The specific CDD obligations for a DNFBP, under the AML Regulations and AML Code are, inter alia, to:

    a) Establish and maintain written policies, procedures, processes, and controls in respect of CDD measures, which should form part of its overall AML compliance manual.

    b) Establish and communicate its policies, procedures, processes, and controls to all relevant employees.

    c) Establish an ongoing employee training program to ensure that relevant employees are kept informed of changes to written policies, procedures, processes, and controls, as well as new developments, including information on current money laundering and terrorist financing risks, techniques, methods, and trends.

d) Identify, verify, and assess clients before establishing a business relationship or carrying out an occasional transaction for them.

e) Ascertain the purpose and nature of the intended business relationship.

f) Ascertain the type, volume, and value of a customer's expected activity.

g) Ascertain the reason for using a DNFBP based in the TCI, unless the customer is resident in the TCI.

h) Determine if a client is acting for a third party and applying the same steps in (e) and (f) above on the third party.

i) Assess the money laundering and terrorist financing risks presented by any client based on the type of customer, the countries with which customers are connected, the products and services that the DNFBP provides or offers to provide to customers, and how the DNFBP delivers its products and services to customers.

j) Establish the source of the funds presented by customers and, where necessary, their source of wealth.

k) Keep specific records for a minimum period of five years.

l) Records relating to customer transactions should contain the following information concerning each transaction carried out:
   - the full name and address of the customer
   - if the transaction is a monetary transaction, the currency and the amount of the transaction
   - if the transaction involves a customer's account, the number, name or other identifier for the account
   - the date of the transaction
   - details of the counterparty, including account details
   - the nature of the transaction
   - details of the transaction and
   - any conclusions reached from an examination of any unusual, or higher risk activity or transaction, which focused on determining the background and purpose of the activity or transaction.

m) Records are to be kept in such manner that:
   - facilitates ongoing monitoring, and periodic updating of, these records
   - ensures that they are readily accessible to the DNFBP in the TCI
   - enables the Commission, internal and external auditors, and other competent authorities, to assess the effectiveness of systems and controls that are maintained by the DNFBP to prevent and detect money laundering and the financing of terrorism.

n) Where records are kept other than in legible form, they must be kept in such manner

that enables them to be readily produced in the TCI in legible form.

o) Carry out ongoing monitoring of customers.

CUSTOMER DUE DILIGENCE (CDD) MEASURES

What is CDD?

11. CDD is information which comprises of the facts about a customer (customer identification information) and the business relationship being entered. CDD information should enable a DNFBP to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering and terrorist financing.

12. The customer identification process requires DNFBPs to take appropriate steps to establish a reasonable belief that all customers - for whom they carry out a transaction or enter a formal business relationship with - are who they say they are. The collection of customer identification and the verification process of the identification submitted, allow a DNFBP to determine its customers' money laundering and terrorist financing (ML/TF) risk profile, as well as whether:

    a) A customer, any third party for whom the customer is acting, and any beneficial owner of the customer or third party, is a politically exposed person (PEP).

    b) A business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations, or is from countries for which there is a call to apply enhanced or countermeasures by the FATF, UN or EU.

    c) A business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that is subject to measures for purposes connected with the prevention and detection of money laundering or terrorist financing, imposed by one or more countries, or sanctioned by the UN or EU.

13. DNFBPs are also required to obtain relationship information. Relationship information is information concerning the business relationship, or proposed business relationship, between the DNFBP and the customer. The business relationship information that DNFBPs are required to ascertain include information set out in Table 1 below.

14. Relationship or transaction information should be obtained for all customers regardless of the extent of CDD measures applied to them, based on their risk assessment (ie whether the customer is assessed as presenting a lower or higher level of risk.)

15. While CDD is undertaken for AML purposes, there are other sophisticated analysis which

CDD can facilitate including market segmentation, customer segmentation, among others. Taking a more strategic approach to business decisions regarding marketing resources and the maximization of cross- and up-selling opportunities for example, could result in DNFBPs achieving their business goals such as increased sales. DNFBPs can maximize sales if they know as much about their customers as possible.

Table 1: CDD Information (Customer Information vs Relationship/Transaction Information)

Customer Information	Relationship Information
Full name (including any former names and aliases).	The purpose and intended nature of the business relationship or occasional transaction.
Gender.	The type, volume, and value of the expected activity.
Date of birth.	The source of funds and - where the customer risk assessment indicates that the customer, business relationship or occasional transaction presents a high risk - the source of wealth of the customer, third party or beneficial owner, both of which are discussed further below.
Nationality.	Details of any existing relationships with the DNFBP.
Principal residential address.	Unless the customer is resident in the TCI, the reason for using a DNFBP based in the TCI.
Valid, official government-issued identity number or other government identifier.	Such other information concerning the relationship that, on a risk-sensitive basis, the DNFBP considers appropriate.

Why is it important for a DNFBP to know its customer?

16. A DNFBP must know its customer for the following reasons, inter alia:

a) To enable the DNFBP to be reasonably certain that its customers/clients are who they say they are, and that it is appropriate to provide them with the products or services requested.

b) To guard against fraud, including impersonation and identity fraud.

c) To help the DNFBP develop a ML/TF risk profile of its customers to identify during a continuing relationship what is unusual, and to enable the unusual to be examined. If unusual events do not have a commercial or otherwise straightforward reasoning, they may involve money laundering, fraud, or support of terrorism.

d) To enable the DNFBP to assist law enforcement by providing available information on customers/clients being investigated, following the filing of a suspicion activity report (SAR) to the Financial Intelligence Agency (FIA).

e) To comply with the requirements of international standards (such as the FATF 40 Recommendations), the AML Regulations, AML Code and its Guidance Notes

When is it necessary to determine the identity of your customer?

17. A DNFBP must identify the customer and verify the identity of the customer when:

a) The customer wishes to establish a business relationship or to carry out an occasional transaction.

b) There is a suspicion of money laundering or terrorist financing.

c) There are doubts about the veracity or adequacy of previously obtained customer documents, data, or information.

d) Conducting on-going monitoring.

e) Completing a transaction for a high-risk customer, eg non-resident customer/client, PEP or other.

18. Generally, DNFBPs are required to conduct CDD on their customers/clients before the establishment of a business relationship with them, and no work or transactions should be undertaken until the CDD is completed. However, a component of CDD - the verification of the identity of a customer, third party or beneficial owner - may be delayed until after the establishment of a business relationship under the AML Regulations. While the Commission strongly encourages DNFBPs to verify the identity of potential customers before establishing a business relationship with them, or carrying out an occasional transaction for them, DNFBPs can delay the verification of the identity of a customer, third party or beneficial owner if the following conditions exist:

a) it is necessary in order not to interrupt the normal conduct of business

b) there is little risk of ML or TF and these risks are effectively managed, and

c) verification of identity is completed as soon as reasonably practicable after the contact with the customer is first established.

19. There should be strict controls where identity verification is delayed, including regular tracking and reporting to senior management to ensure that identity verification is completed. It is important to restrict customer activity during this period; outward/inward payments should not be permitted until the customer's identity verification requirements are satisfied. If it is not possible to complete customer identity verification in a timely manner, the DNFBP must terminate the business relationship with the customer. The DNFBP should also consider whether it is appropriate to file a SAR with the FIA. Most importantly, the DNFBP must ensure that it does not tip-off the customer where a SAR is being filed, ie expose to the customer, the target of the SAR, that suspicions have been formed and are being reported to the FIA.

20. The information set out from paragraphs 23 to 35 of this guidance, which a DNFBP is required to obtain from potential or actual customers, should be obtained through a standard customer information form, ie a template which will ensure consistency in the information

obtained for all its customers.

21. Additionally, DNFBPs that offer services to customers should ensure that they establish a customer agreement for each business relationship. The customer agreement should define the relationship, the responsibilities of each party, the compensation or payment, the services that will be provided, the timeframe for delivering the services (if applicable) and how the agreement can be terminated, among other things.

What should a DNFBP do if it is unable to verify the identity of a customer, or if it is unable to obtain sufficient information about the nature or purpose of a transaction?

22. A DNFBP **must not** carry out a transaction for or enter a business relationship with that customer, and **must terminate** any business relationship already established, and consider submitting a SAR to the FIA. See details on how to file a SAR further below.

Identifying and verifying the identity of a customer who is a natural person

23. A DNFBP should identify a customer who is a natural person by obtaining their full name (including any former names and aliases), principal residential address, gender, date of birth and nationality based on documents, data or information obtained from a reliable and independent source. In respect of natural persons, much weight is placed on valid government-issued, photo-based identity documents (eg passports), as these are often the easiest way of being reasonably satisfied of someone's identity. More importantly, a passport is arguably not easily forged since it is issued after a due diligence check.

24. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of valid, government-issued, photo-based identity (eg a driver's license or national identity card, which bears a clear photograph of the customer and which usually bears his signature.) If a customer holds dual nationality, DNFBPs should consider whether this has an impact on the customer's ML/TF risk profile. For further information, DNFBPs should refer to the Commission's Anti-Money Laundering and Prevention of Terrorism Risk Assessment Guidelines of August 2020.

25. DNFBPs must obtain additional identification for customers that presents a higher level of risk. The additional information must include the customer's place of birth, nationality and an official government-issued identity number or other government identifier. In respect of higher risk customers, DNFBPs are only required by the AML Code to verify the customer's full legal name, any former names, and any other names **and either**, the principal residential address of the customer **or** the customer's date of birth.

26. While DNFBPs must ascertain the principal residential address of a customer, verification of this information is only required for customers that present a higher level of risk. The

Commission considers the following methods of verifying an individual's principal residential address to be acceptable (either/or):

a) a bank statement or a utility bill, dated within the last three months, in the customer's full name (ie the name as per the bank statement or utility bill submitted) capturing a physical residential address (not a correspondence address, eg PO Box number)

b) correspondence from a central or local government department or agency

c) a letter of introduction confirming customer's residential address from a regulated person, a foreign regulated person, or the owner, manager or operator of the residence

d) confirmation of address from an employer or a connected institution

e) a personal visit to the individual's residential address and a file note capturing the details of that home visit.

Identifying and verifying the identity of a customer who is a legal person

27. A DNFBP must identify a customer who is a legal person (company) and legal arrangements (partnerships or unincorporated entities). The type of information needed to identify a customer who is a legal person or legal arrangement, includes:

a) Name, legal form, and proof of existence, verified by a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust or other documentation from a reliable independent source proving the name, form and current existence of the customer.

b) The powers that regulate and bind the legal person or arrangement (eg the articles of incorporation of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (eg senior managing directors of a company, trustees of a trust).

c) Understanding the nature of its business, its ownership, and its control structure.

d) The registered office address and the principal place of business (if different) which may be verified by a company search, articles of incorporation, statement from the Registered Agent, or similar.

28. A DNFBP should also identify and take reasonable steps to verify the identity of the natural person(s) owners who own or control 10% or more of the customer.

29. In respect of higher risk customers that are a legal entity, DNFBPs must also obtain identification information on every director or person occupying a senior management position (eg chief executive, operating, risk officers etc or any other officer who holds a position that has the authority to bind the licensee in a contract) in the legal entity. Where identification information on an individual, as a director, senior manager or beneficial owner of the legal entity is required to be obtained, the process set out in paragraphs 20 to 23 of this

guidance apply.

Identifying and verifying the identity of a customer that is a trust

30. The type of information needed to identify a customer that is a trust, includes:

i) the name of the trust

ii) the date of the establishment of the trust

iii) any official identifying number (if applicable)

iv) identification information on each trustee of the trust

v) the mailing address of the trustees

vi) identification information on each settlor of the trust

vii) identification information on each protector or enforcer of the trust (if applicable)

viii) identification information on each beneficiary with a vested right and each beneficiary or each person who is an object of a power

ix) the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control or ownership.)

31. The above information can be verified through the trust agreement. Verification of the identity of the trustees, the protector or enforcer, the settlor, beneficiaries with a vested right and beneficiaries that are objects of a power, must follow the measures set out for individuals and legal persons in paragraphs 20 to 23 and paragraphs 24 to 26, respectively.

32. If a DNFBP determines that any business relationship or occasional transaction concerning the trust that the DNFBP is required to identify, presents a higher level of risk, the DNFBP must obtain any additional identification information it considers appropriate.

Identifying and verifying the identity of a customer that is a foundation

33. The type of information needed to identify a customer who is a trust, includes:

a) the full name of the foundation

b) the date and country of the establishment, registration, formation, or incorporation of the foundation

c) any official identifying number

d) the registered address (or equivalent) of the foundation or, if the foundation does not have a registered address (or equivalent), the address of the head office of the foundation

e) the mailing address of the foundation, if different from its registered address (or equivalent)

f) the principal place of business of the foundation, if different from its registered address (or equivalent)

g) the name and address of the registered agent of the foundation, if any

h) the name and address of the secretary, or equivalent, of the foundation, if any

i) the names of the foundation council members (or equivalent) and, if any decision requires the approval of any other persons, the names of those persons

j) identification information on those foundation council members (or equivalent) who have authority to give instructions to the financial business concerning the business relationship or occasional transaction

k) identification information on the guardian of the foundation (or equivalent), if any and

l) identification information on the founder or founders, on any other person who has contributed to the assets of the foundation, and on any person to whom the rights of the founder or founders have been assigned.

34. The above information may be verified through the foundation's constitution or official registration documents. If a DNFBP determines that any business relationship or occasional transaction concerning the foundation that it is required to identify, presents a higher level of risk, the DNFBP must obtain any additional identification information it considers appropriate.

35. It is important to note that where a DNFBP enters a business relationship with, or carries out an occasional transaction for, a customer who acts on behalf of another person, the DNFBP must always establish the identity of the person on whose behalf or benefit that customer acts.

Use reliable sources of documentation to verify identify

36. It is important that DNFBPs only rely on information from reliable independent sources to verify identity, or the nature and existence of the legal person or legal arrangement. The original identity document should be obtained by the DNFBP as a matter of preference; however, if it is not possible to obtain the original document, then certified copies must be obtained. The certified copies of the original identity document must be legible and certified as "original seen" by a suitable certifier. Uncertified copies of copies should never be accepted.

Source of Funds (SOF)

37. Source of Funds (SOF) relates to the business, transaction or other activity that generates the funds relevant to the current transaction, which may include the customer's occupation. A DNFBP should take reasonable steps, consistent with the ML/TF risk profile of the customer

and the nature of the business relationship, to identify the source of funds of all its customers. DNFBPs are strongly encouraged to verify source of funds on a risk-sensitive basis. If a customer's ML/TF risk profile is not low risk, the DNFBP should verify the source of the customer's funds using reliable, independently sourced documents, data, or information, and keep appropriate records of the same.

Customer screening

38. Customer screening is an important part of a DNFBP "knowing its customer". Screening of the customer's full name must be conducted before the commencement of a business relationship or an occasional transaction, and on an on-going basis.

39. The primary purpose of customer screening is to ensure that a DNFBP does not conduct business with individuals or organisations named on sanctions lists. In addition, DNFBPs should consider checking for other information which may influence a customer's ML/TF risk profile (eg media reports may be useful in developing a more complete profile of a customer.) Often, commercial databases will provide this information in addition to sanctions checking and monitoring.

40. The Commission regularly circulates financial sanctions notices (FSNs) identifying targets of sanctions programs. Additionally, the UK Office of Financial Sanctions Implementation (OFSI) maintains a consolidated list of sanctions targets which is searchable via its website. This OFSI search tool provides a cost-free method for customer name-screening against UK-issued sanctions. All DNFBPs must ensure that potential customers are subject to screening and existing customers should be screened against each FSN circulated by the Commission, and more generally on a risk-sensitive basis. The FSNs circulated by the Commission can be found here.

Prohibited Relationships

41. The AML Regulations and AML Code set out circumstances which constitute prohibited relationships, such as correspondent banking relationships with shell banks, the set-up of anonymous, numbered accounts, or the set-up of accounts in a name which are known or suspected to be fictitious.

42. All DNFBPs must pay special attention to services, products or transactions that may allow anonymity and take additional measures to prevent their use in money laundering or terrorist financing activity. DNFBPs should include any such service, product, or transaction within those requiring enhanced due diligence.

43. In addition, DNFBPs must comply with any prohibition issued through orders made by the UK (communicated through the TCI Attorney General's Chambers in the form of Financial Sanctions Notices and the OFSI Consolidated List) in respect of sanctioned persons, or where

the Financial Action Task Force (FATF)/CFATF has called for countermeasures or enhanced measures to be taken against countries with material deficiencies in their anti-money laundering and counter financing of terrorism (AML/CFT) regimes. The Commission issues advisory notices stipulating that DNFBPs, among others, exercise caution when entering business relationships involving customers from such countries. Please see the Commission's in-depth report on the financial sanctions survey conducted in April and May of 2020, found here.

Extent of CDD

44. The DNFBP must ensure that the CDD measures taken in respect of a customer are adequate and address the ML/TF risks presented by the customer. The CDD steps that a DNFBP takes will depend upon the ML/TF risk profile of the customer. Assessment of a customer's ML/TF risk profile is discussed in detail in the Commission's Anti-Money Laundering and Prevention of Terrorism Risk Assessment Guidelines of August 2020. Where a customer is assessed as low risk, the DNFBP may consider implementing a reduced due diligence framework or Normal or Regular Due Diligence (RDD). For higher risk customers, the DNFBP is required to take more detailed steps to know and understand the customer or Enhanced Due Diligence (EDD).

Simplified Due Diligence (SDD)

45. The AML legislation provides for the following SDD measures:

- adjusting the amount of customer and relationship information required for verification – refer to appendices 1 to 3 for a list of the reduced information to be obtained for low-risk customers
- adjusting the source of identification verification documents e.g., accepting verification documents from one independent source rather than two as is required for customers with a higher level of risk
- adjusting the frequency of CDD reviews of the business relationship.

46. The FATF Recommendation 1 requires countries to identify, assess, and understand their money laundering and terrorist financing risks before allowing DNFBPs and other financial businesses to apply simplified measures. This is to ensure that the simplified measures are commensurate with the ML/TF risks identified by respective countries.

47. The TCI's National Risk Assessment (NRA) identified the domestic insurance sector as low-risk, and as such, SDD measures should apply to customers that are domestic insurers. No other sector was identified as low risk. Additionally, the NRA did not consider the ML/TF risk of other types of customers such as public authorities, or corporations whose shares are traded on the securities exchange. While these types of customers are universally perceived as

having a low level of ML/TF risk and are prime candidates for SDD, the TCI's NRA did not provide an assessment of those types of customers.

48. Steps are being taken to reconcile the FATF Recommendations on SDD with the relevant provisions in the TCI legislation.

49. It is important to appreciate that identifying a customer as carrying a lower risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is not a money launderer or is not financing terrorism.

Normal/Regular Due Diligence (NDD/RDD)

50. If a customer is assessed as presenting a lower level of ML/TF risk, a DNFBP may decide to conduct Normal or Regular Due Diligence (RDD). RDD should not be conducted where there is a suspicion of money laundering or terrorist financing. If there is a significant change to the business of a customer subject to RDD, the DNFBP should review the customer's ML/TF risk profile, and if necessary, upgrade the Client Due Diligence carried out to ensure that it is appropriate to the changed circumstances.

51. Examples of RDD measures include adjusting the:

    a) amount of information required for verification as indicated in paragraphs 16 and 19 above

    b) frequency of CDD reviews of the business relationship

    c) frequency and intensity of transaction monitoring.

52. It is important to appreciate that identifying a customer as carrying a lower risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is not a money launderer or is not financing terrorism.

Enhanced Due Diligence (EDD)

53. If a customer is assessed as presenting a higher level of money laundering and/or terrorist financing risk, the DNFBP must conduct EDD. In addition, the DNFBP must conduct EDD if a customer has been identified as high risk in the TCI's National Risk Assessment.

54. The AML Code identifies the following situations as automatically high risk:

    a) Non-face-to-face business relationships

    b) Customers, third parties, beneficial owners that are PEPs

55. Examples of EDD measures include:

a) verification of information by using multiple reliable and independent sources

b) obtaining additional information on a customer (eg occupation, amount of assets, information from public databases, internet searches etc) and more regularly updating the identification data of the customer and beneficial owners

c) obtaining additional information on the intended nature of the business relationship

d) obtaining information on the source of wealth of a customer

e) obtaining information about the reasons for proposed transactions or transactions that have already been undertaken

f) seeking senior management approval to commence or continue a business relationship, and

g) enhanced monitoring of the business relationship by increasing the number and timing of controls and selecting types or patterns of transactions that need further review.

56. It is important to appreciate that identifying a customer as carrying a higher risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is a money launderer or financing terrorism.

Source of Wealth (SOW)

57. A person's "source of wealth" (SOW) means the business, transactions or other activities that have generated the total net worth of a person. It should be noted that it is the source of the person's wealth that is important rather than the amount of it. It may not, therefore, be necessary for information on the amount of wealth to be obtained.

58. The AML Regulations and AML Code require SOW to be obtained for higher risk customers. Similar to SOF, TCI law currently does not require a DNFBP to verify the SOW of its customers. However, DNFBPs are strongly encouraged to verify SOW using reliable, independent source documents, data, or information, and to keep appropriate records of the same.

***Table 2**: Simplified Due Diligence (SDD) information vs Enhanced Due Diligence (EDD) information*

SDD information applicable to Lower Risk Customers (Individuals)	Verification Required	**EDD information applicable to Higher Risk Customers (Individuals)**	Verification Required
Full name	Yes	Full name	Yes
Gender	Yes	Gender	Yes
Date of birth	Yes	Date of birth	Yes
Nationality	Yes	Place of birth	Yes
Principal residential address	No	Nationality	Yes
SOF	No	Official government-issued	Yes

		identity number or other government identifier	
SOW	No	SOF	Yes
		SOW	Yes

How to determine the extent of CDD - the Customer Risk Assessment

59. A risk-sensitive approach to CDD requires a risk assessment to be undertaken with respect to a particular customer, based on that customer's individual circumstances, ie the customer's information and the relationship information. This will determine the extent of the identification and other customer due diligence information that will be sought, how it will be verified, and the extent to which the resulting relationship will be monitored.

60. The broad objective of a risk-sensitive approach (the RBA) is to enable a DNFBP to target resource and effort where the risk is greatest and, conversely, reduce requirements where the risk is low. This is achieved by the DNFBP preparing a ML/TF risk profile for each customer based on the following factors:

a) its customers

b) the jurisdictions to which its customers are connected

c) the products and services offered

d) the mechanism through which the business relationship is commenced and transacted with the customer, and

e) any other relevant factors.

Table 3: Indicators of higher risk situations based on the standard risk categories

Customer Risk	Country Risk	Product/Service Risk	Delivery Channel Risk
Politically exposed person	Customers from countries that have inadequate safeguards in place against money laundering or terrorist financing	Products offered to a customer by the DNFBP that involves the ability to make payments to third parties	Where the relationship with the customer is indirect, for example using intermediaries
Complex business structures, for example structures involving a mixture of companies and trusts or simply several different companies	Customers from countries that have high levels of organised crime	Products/services involving the ability to pay in or withdraw cash	Non-face to face relationships, for example where products are delivered exclusively by post or telephone or over the Internet
Customers that use bearer shares	Customers from countries that have strong links with terrorist activities	Ability to migrate from one product to another	
Customers that generate	Customers from	Ability to hold boxes,	

Customer Risk	Country Risk	Product/Service Risk	Delivery Channel Risk
significant amounts of cash, or with a high value of funds	countries that are vulnerable to corruption	parcels, or sealed envelopes in safe custody	
Where there is no clear rationale for the customer purchasing your product or service	Customers from countries that are the subject of United Nations or European Union sanctions	Ability to use numbered accounts or accounts that offer a layer of opacity	
Where the customer requests unusual levels of secrecy with a transaction or the relationship or, in the case of a legal entity, reluctance to provide information as to beneficial owners or controllers		Ability to pool underlying customers	
Situations where the source of funds and/or the origin of wealth cannot be easily verified			
Delegation of authority by the customer, for example, through a power of attorney			

Updating CDD

61. The AML Regulations require a DNFBP to update CDD information (customer information and relationship information) where the DNFBP:

    a) suspects money laundering or terrorist financing

    b) doubts the veracity or adequacy of documents, data or information previously obtained under its customer due diligence measures or when conducting ongoing monitoring

    c) at other appropriate times to existing customers as determined on a risk-sensitive basis.

62. Where CDD is to be updated on a risk-sensitive basis, a DNFBP is expected to:

    a) review and update customers' due diligence information on at least an annual basis where it has assessed a customer relationship as presenting a higher risk, and

    b) review and update customers' due diligence information on a risk-sensitive basis, but not less than once in every five years, where it has assessed a customer relationship as presenting a normal or low risk.

63. Events such as the opening of a new account, the purchase of a further product, or meeting with a customer may present a convenient opportunity to update customer due diligence information.

Relying on CDD conducted by third parties

64. DNFBPs may rely on introducers and intermediaries to apply CDD measures with respect to a customer, third party or beneficial owner, if:

a) the introducer or intermediary is a regulated person or a foreign regulated person; and

b) the introducer or intermediary consents to being relied on.

65. Before relying on an introducer or intermediary to apply customer due diligence measures with respect to a customer, third party or beneficial owner, DNFBPs must obtain adequate assurance in writing from the intermediary or introducer that:

a) the intermediary or introducer has applied the CDD measures for which the financial business intends to rely on it

b) the intermediary or introducer is required to keep, and does keep, a record of the evidence of identification relating to each of the customers of the intermediary or introducer

c) the intermediary or introducer will, without delay, provide the information in that record to the financial business at the financial business's request

d) the intermediary or introducer will, without delay, provide the information in the record to the Commission, where requested by the Commission, and

e) the intermediary understands and obtained information on the purpose and intended nature of the business relationship.

66. DNFBPs must consider whether an introducer or intermediary is regulated and supervised, or monitored, and has measures in place for compliance with customer due diligence and record keeping requirements. DNFBPs must also take into consideration the level of risk of countries in which the introducer or intermediary financial business is located.

67. The DNFBP and its senior management remain responsible for the proper conduct of CDD and ongoing monitoring for its customers.

Independent Audits

68. An AML/CFT Independent Audit remains a vital element of any effective Compliance Program for DNFBPs. The AML legislation requires DNFBPs to maintain an adequately independent audit function to test compliance (including sample testing) with their AML policies, systems and controls, and the effectiveness of its employees' AML/CFT awareness

and the training provided to them.

69. While the frequency of audit is not specifically defined in the AML legislation, a sound practice is for DNFBPs to conduct independent testing generally every 12 to 18 months, commensurate with its policies, procedures, and anti-money laundering risk profile.

70. The persons conducting the AML testing should report directly to the board of directors. The board of directors should ensure that the persons conducting the AML testing do not present a conflict of interest or lack of independence.

71. Independent audit testing of customer due diligence should, at a minimum, include:

- Reviewing the adequacy and comprehensiveness of KYC/CDD policies and procedures to determine whether they are aligned to internal processes and cover the applicable regulatory requirements.
- Performing walkthroughs to understand the knowledge and experience of staff responsible for onboarding customers.
- Reviewing the customer-risk rating methodology and processes.
- Reviewing a sample of new accounts opening from operating effectiveness.
- Reviewing and testing of high-risk accounts and periodic high-risk review processes.
- An evaluation of the overall adequacy and effectiveness of the Customer Due Diligence program, including policies, procedures, and processes.
- A review of DNFBP risk assessment for reasonableness given DNFBP risk profile (products, services, customers, entities, and geographic locations).
- Appropriate risk-based transaction testing with respect to the customer profile to verify a DNFBP adherence to its policies and procedures, record keeping, and reporting requirements.
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations.
- A review of staff training for adequacy, accuracy, and completeness.
- An assessment of the integrity and accuracy of the Management Information System (MIS) used.

Red Flags for CDD

72. When conducting CDD, DNFBPs should be alert to unusual behaviour by a customer or unusual circumstances that may require further investigation. If the DNFBP remains suspicious after conducting those investigations, it should consider whether it is appropriate

to commence or continue a business relationship. The DNFBP should also consider whether it is appropriate to file a SAR with the FIA. Moreover, the DNFBP must ensure that it does not tip-off the customer.

73. Examples of unusual customer behaviour include where the customer:

a) is secretive or evasive about who they are, the reason for the transaction, or the SOF

b) uses an intermediary, or does not appear to be directing the transaction, or appears to be acting as a front for an undisclosed controller or Ultimate Beneficial Owner (UBO)

c) avoids personal contact without good reason

d) refuses to provide information or documentation, or is unable to provide it or needs to refer to a third party, or the documentation provided is suspicious

e) has criminal associations, known or suspected

f) has an unusual level of knowledge about ML processes, or

g) does not appear to have a business association with the other parties to a transaction but appears to be connected to them.

74. Examples of unusual circumstances concerning SOF include:

a) large cash payments

b) unexplained payments from a third party

c) large private funding that does not fit the business or personal profile of the payer

d) loans from non-institutional lenders

e) use of corporate assets to fund private expenditure of individuals

f) use of multiple accounts or foreign accounts from high-risk jurisdictions.

Reporting Suspicious Activity

75. Officers or employees of a DNFBP must promptly make a SAR to the DNFBP's MLRO where they know, suspect, or have reasonable grounds to suspect ML or TF, or that funds are any of the following:

a) the proceeds of crime

b) related to terrorism financing

c) linked, or related to, or are to be used for, terrorism, terrorist acts, or by terrorist organisations.

76. The legal obligation on officers and employees of a DNFBP to make a SAR, as above, applies even where a business relationship or transaction does not proceed.

77. The MLRO is responsible for receiving, assessing, and deciding, whether to make a disclosure to the FIA about internal reporting of suspected suspicious activity.

78. A decision whether to submit a SAR to the FIA is solely the MLRO's responsibility. The MLRO must consider all the information available and may submit a SAR to the FIA even when no internal reporting has been made. All SARs must be made in good faith.

79. A DNFBP must ensure that it does not tip-off a customer when it makes a SAR.

80. The Commission will soon publish its Suspicious Activity Reporting Guidance which readers are strongly encouraged to read. The guidance aims to help financial businesses comply with suspicious activity reporting obligations by specifying when reports must be made, in what circumstances, what details to include, and how to report them.

What is "Tipping-Off"?

81. Tipping-off, in relation to a potential customer or a customer of a DNFBP, is the unauthorized act of disclosing information that may result in the potential or actual customer, or a third party (other than the FIA or the Commission), knowing or suspecting that a SAR has been filed. Care should be taken to ensure that the customer does not become aware (i.e. is not tipped off) about the reporting of suspicion.

82. Tipping-off may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorism financing.

83. If a DNFBP is in the process of carrying out a transaction for a customer that becomes subject to a SAR before the transaction has been completed, consent to complete the transaction must be obtained from the FIA.

APPENDIX 1: Customer Information to be obtained based on customer ML/TF risk profile

ML/TF Risk Profile	Full name	Former names	Gender	Date of birth	Place of birth	Nationality	Principal residential address	Official government-issued identity number or other government identifier	Source of funds	Source of wealth
Low Risk Customer	√	√	√	√	x	x	√	x	√	x
Medium Risk Customer	√	√	√	√	√	√	√	x	√	x
High Risk Customer	√	√	√	√	√	√	√	√	√	√

APPENDIX 2: Customer Information to be verified based on customer ML/TF risk profile

Customer ML/TF Risk Profile	Full name	Former names	Gender	Date of birth	Place of birth	Nationality	Principal residential address	Official government-issued identity number or other government identifier	Source of funds	Source of wealth
Low Risk Customer	√	√	x	Not required if address is verified	x	x	Not required if date of birth verified	x	x	x
Medium Risk Customer	√	√	√	√	√	√	√	x	x	x
High Risk Customer	√	√	√	√	√	√	√	√	√	√

APPENDIX 3: Relationship Information to be obtained based on customer ML/TF risk profile

ML/TF Risk Profile	Purpose/intended nature of the business relationship	Type of expected activity	Volume of the expected activity	Details of any existing relationships	Reason for using a TCI business (non-resident customers)	Source of funds	Source of wealth
Low Risk Customer	√	√	√	√	√	√	x
Medium Risk Customer	√	√	√	√	√	√	x
High Risk Customer	√	√	√	√	√	√	√

APPENDIX 4: GENERAL REQUIREMENTS RELATING TO DNFBPs

As a DNFBP, the general obligations under the AML Regulations and AML Code are to:

1. Register with the DNFBP Supervisor (the Commission)
2. Provide updated information to the DNFBP Supervisor on a periodic basis
3. Appoint a Money Laundering Compliance Officer (MLCO)
4. Appoint a Money Laundering Reporting Officer (MLRO)
5. Develop an effective Compliance Program
6. Identify clients before establishing a business relationship or carrying out an occasional transaction for them
7. Verify the identity of clients before establishing a business relationship or carrying out an occasional transaction for them
8. Determine if a client is acting for a third party and applying the same steps in 6 and 7 above
9. Assess the money laundering and terrorist financing risks presented by any client based on the type of customer, the countries with which customers are connected, the products and services that the DNFBP provides or offers to provide to customers, how the DNFBP delivers its products and services to customers
10. Establish the SOF presented by customers and, where necessary, source of customers wealth
11. Keep specific records for a minimum period of five years as further explained in this guidance
12. Carry out on-going monitoring of customers and their transactions
13. Submit SARs to the FIA and avoid "tipping-off" – see guidance issued by the Commission on Suspicious Activity Reporting here
14. Carry out independent audit to test the DNFBPs compliance with their policies, systems, and controls.