THE TURKS AND CAICOS ISLANDS
FINANCIAL SERVICES COMMISSION

GUIDANCE FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS WHEN PREPARING ANTI-MONEY LAUNDERING AND PREVENTION OF THE FINANCING OF TERRORISM AND PROLIFERATION POLICIES AND PROCEDURES ("AML MANUAL")

11 September 2023

TURKS AND CAICOS ISLANDS FINANCIAL SERVICES COMMISSION GUIDANCE FOR PREPARING ANTI-MONEY LAUNDERING/ANTI-TERRORISM AND PROLIFERATION FINANCING (AML/ATF) POLICIES AND PROCEDURES

NOTE: This is guidance for Designated Non-Financial Businesses and Profession's (DNFBP) in preparing Anti-Money Laundering, and Prevention of Terrorist Financing and Proliferation Financing (AML/PTF) policies and procedures, hereinafter referred to as AML Manual. This document is guidance and should not be considered to be legal advice. The document outlines the issues that should be addressed in a DNFBP's AML Manual.

DNFBP Full Name

Address | Telephone | Email

TABLE OF CONTENTS

GLOSSARY OF TERMS

AML/PTF	AML means Anti-Money Laundering and CFT means Prevention of Terrorist Financing.
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
Customer Due Diligence (CDD)	CDD includes; • Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from customer or through reliable and independent source. • Identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures to verify his identity so that the financial business is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement. • Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship. • Monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the financial business's knowledge of the customers, their business and risk profile, including, where necessary, the source of funds and, updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with the financial business.
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.
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.
Non-Face-to-Face	Describes a transaction that take place without a customer having to be physically present.
Ongoing monitoring	Ongoing monitoring means: • 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. • 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.
Proliferation Financing	Proliferation Financing ("PF") is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials(including both technologies and dual-used goads for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services, or expertise.
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.

PRODUCTS AND SERVICES IN SCOPE OF AML/PTF REGULATIONS AND CODE
(Schedule 2 of the AML/PTF Regulations)

Provide a brief description of the purpose of your business, including its products and services that are in the scope of the Ant-Money Laundering and Prevention of Terrorist Financing Regulations (the "AML/PTF Regulations") and the Anti-Money Laundering and Prevention of Terrorist Financing Code (the "AML/PTF Code").

YOUR SECTOR/INDUSTRY ML/TF/PF RISKS AND VULNERABILITIES

Provide a brief description of the money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks and vulnerabilities that affect your industry/sector. This information can be found in –

- the TCI's National Risk Assessment;
- sectoral risk assessments conducted by the Financial Services Commission (Commission);
- guidance documents issued by the Commission or the international standard-setting body, the Financial Action Task Force (FATF).

YOUR BUSINESS RISK ASSESSMENT
(Regulation 4 of the AML/PTF Code)

Describe in the AML Manual the following regarding your policies and procedures:

- the key relevant risks, money laundering or terrorist financing, and vulnerabilities faced by your business in its day-to-day operations;
- the likelihood of each risk affecting the business;
- the policies, procedures, and controls in place to mitigate these risks;
- how often the business risk assessment will be reviewed and updated.

KEY POINT

National risk assessments ("NRAs") and Sectoral risk assessments ("SRAs") give a view of ML/TF/PF risks within an entire sector (e.g., independent legal professionals) which may or may not exist in individual institutions. NRAs and SRAs assist DNFBPs in carrying out a business level risk assessment so that they can understand both the general threats that the TCI faces, as well as those specific to the particular areas of work that they carry out. Additionally, the NRA or SRA identify emerging threats that financial businesses should be aware of.

A business risk assessment is specific to a single DNFBP. It is designed to evaluate the money laundering risk associated with a particular financial business.

POLICIES, PROCEDURES, SYSTEMS AND CONTROLS

(Regulation 17 of the AML/PTF Regulations, Regulation 6 of the AML/PTF Code)

Describe and/or include in the AML Manual the following regarding your policies and procedures:

i) A definition of money laundering, terrorist financing and the financing of proliferation.

ii) The role of the money laundering compliance officer (MLCO)
- To oversee and monitor the DNFBPs' compliance with the Proceeds of Crime Ordinance, all legislation in force concerning money laundering and terrorist financing, the AMLPTF Regulations and the Code

iii) The role of the money laundering reporting officer (MLRO)
- To receive and consider internal money laundering and terrorist financing disclosures (suspicious activity report);
- To consider whether a suspicious activity report should be made to the Financial Intelligence Agency; and
- Where he/she considers a suspicious activity report should be made, submitting the report.

iv) How the policies, procedure, systems, and controls will be communicated to employees, branches and subsidiaries

v) How changes to AML/PTF legislative and regulatory requirements will be addressed

vi) How often policies and procedures will be updated and what will influence this updating – financial businesses should be mindful of their AML/CFT obligation to monitor and test the effectiveness of policies and procedures as well as for employee training on the financial business policies and procedures

vii) How often an independent audit of the AML/PTF compliance program will be conducted – reference can be made to the person that will perform the audit and who within the financial business will approve the auditor (e.g. senior management, the board, etc.)

viii) When and what transaction limits will be imposed

ix) When management approvals will be required

x) Who can make changes to the AML Manual

xi) The date that the manual was updated should always be stated

CUSTOMER ACCEPTANCE POLICY

(Regulation 6 of the AML/PTF Code)

Describe in the AML Manual how you will comply with your risk assessment and risk mitigation obligations including:

i) Who will be accepted as a customer? Consider the following –

- Does the customer meet the ML/TF risk appetite established by you?
- Are prospective customers required to sign a customer acceptance agreement agreeing to comply with the CDD measures applied by you at onboarding and after onboarding on an ongoing basis?
- Has the prospective customer complied with your CDD measures?

RISK ASSESSMENT AND RISK MITIGATION

(Regulation 17 of the AML/PTF Regulations, Regulation 4 of the AML/PTF Code)

Describe how the registrant will comply with its risk assessment and risk mitigation obligations including:

ii) Identifying what customers and situations it has identified as higher risk based on its business risk assessment (copy of the risk assessment should be attached to the AML Manual as an appendix).

iii) What mitigation and control measures it will implement to reduce the higher risk?

iv) How will it assess and document the risk of any new products or services?

v) How often it will update its business risk assessment?

CUSTOMER DUE DILIGENCE (CDD)

(Part II of the AML/PTF Regulations, Part 3 of the AML/PTF Code)

Describe in the AML Manual how the registrant will comply with CDD requirements, including:

i) When and how it will identify the customer? Please note that the identity of the customer must be ascertained and verified before starting a business relationship or conducting an occasional transaction, although the law allows a delay in certain situations

ii) What information will be collected when the customer is a natural person?

iii) What information will you collect when the customer is a legal person/legal arrangement?

iv) What identification documents are acceptable?

v) Will copies of documents be accepted; and if yes, how will be the copies be authenticated?

vi) What are the identification procedures, including acceptable documents, for customers who are not physically present?

vii) What will you do if you cannot complete customer due diligence measures?

KEY POINT 1

The AML Manual must include at a minimum, the following identification information in respect of customers that are natural persons:

- Full name (including any former names and aliases);
- Gender;

- Date of birth;
- Nationality; and
- Principal residential address.

The AML Manual must set out how the identification information is to be verified. The document used for verification should be in colour instead of black and white to ensure it is legible. The following documents can be used for verifying identity and address:

- Valid passport (preferred method for identity verification);
- Valid driver's License (used for identification and address verification);
- Utility bill e.g. electricity bill (used for address verification)

The AML Manual must also include, at a minimum, the following information about the business relationship in respect of customers:

- The purpose and intended nature of the business relationship or occasional transaction
- The type, volume, and value of the expected activity
- The source of the funds provided by customers, 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
- Unless the customer is resident in the TCI, the reason for using a DNFBP based in the TCI

NOTE: Additional measures must be taken where the customer has higher risk factors. Refer to the Anti-Money Laundering and Prevention of Terrorist Financing Code and Guidance Notes for more information.

KEY POINT 2

The AML Manual must include at a minimum, the following identification information in respect of customers that are legal entities:

- the full name of the legal entity and any trading names that it uses;
- the date of the incorporation, registration, or formation of the legal entity;
- the registered office or, if it does not have a registered office, the address of the head office of the legal entity;
- the name and address of the registered agent of the legal entity (or equivalent), if any;
- the mailing address of the legal entity;
- the principal place of business of the legal entity;
- the names of the controllers (i.e. directors, senior managers, etc.) of the legal entity along with relevant CDD information.

The AML Manual must set out how the identification information is to be verified. The following documents can be used for verifying identity and address:

- certificate of incorporation, registration or equivalent;
- a company registry search, including confirmation that the legal entity is not in the process of being dissolved, struck off, wound up or terminated;
- the latest audited financial statements of the legal entity;
- independent data sources, including electronic sources, e.g. business information services; and
- where the DNFBP determines that the legal entity does not present a low risk, a personal visit to the legal entity's principal place of business.

NOTE: Additional measures must be taken where the customer has higher risk factors. Refer to the Anti-Money Laundering and Prevention of Terrorist Financing Code and Guidance Notes for more information.

KEY POINT 3

The AML Manual must also include, at a minimum, the following information about the business relationship in respect of customers:

- The purpose and intended nature of the business relationship or occasional transaction
- The type, volume, and value of the expected activity
- The source of the funds provided by customers 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
- Unless the customer is resident in the TCI, the reason for using a DNFBP based in the TCI

NOTE: In light of regulation 16 of the AML/PTF Regulations, the prohibition on entering a correspondent banking relationship with a shell bank and setting up or maintaining a numbered account, an anonymous account or an account in a fictitious name should also be referenced in the AML Manual.

RECORD KEEPING

(Regulations 17 – 19 of the AML/PTF Regulations, Part 7 of the AML/PTF Code)

Describe in the AML Manual how the registrant will comply with record keeping requirements including:

i) How long it will retain records related to the customer, transactions, your AML program?

ii) What records will you retain?

iii) Where will records be retained?

iv) How will the registrant ensure that information can be provided in a timely manner to the Commission, the Financial Intelligence Agency and other law enforcement authorities?

v) If the registrant uses a third party to conduct customer due diligence measures:

- How will it ensure that they are properly identifying customers?
- How will it gain access to information in a timely fashion?

KEY POINT 1

The AML Manual must also include, at a minimum, the following information about the business relationship in respect of customers:

1) The records that must be kept are –

(a) a copy of the evidence of identity obtained pursuant to the application of customer due diligence measures or ongoing monitoring, or information that enables a copy of such evidence to be obtained;

(b) the supporting documents, data or information that have been obtained in respect of a business relationship or occasional transaction, which is the subject of customer due diligence measures or ongoing monitoring;

(c) a record containing details relating to each transaction conducted by the DNFBP during any business relationship or occasional transaction which must contain the following information concerning each transaction conducted—

i) the name and address of the customer;
ii) if the transaction is a monetary transaction, the currency, and the amount of the transaction;
iii) if the transaction involves a customer's account, the number, name, or other identifier for the account;
iv) the date of the transaction;
v) details of the counterparty, including account details;
vi) the nature of the transaction;
vii) details of the transaction; and
viii) any conclusions reached as a result of an examination conducted in relation to suspicious activity reports.

(d) The information required under paragraph 1 (c) of Key Point 1 ought to identify the source and origin of funds.

(e) all account files; and

(f) records concerning suspicious activity, including

i) any internal suspicious activity reports and supporting documentation,
ii) the decision of the MLRO concerning whether to make a suspicious activity report to the Financial Intelligence Agency and the basis of that decision,
iii) details of any reports made to the Financial Intelligence Agency,
iv) records concerning reviews of, and the conclusions reached in respect of complex transactions, unusual large transactions, unusual patterns of transactions, which have no apparent economic or visible lawful purpose; and customers, including natural and legal persons, and transactions

connected with countries which do not apply, or insufficiently apply, the FATF Recommendations or are the subject of UN or EU countermeasures.

(g) records concerning the DNFBPs' policies, systems and controls and training

(h) all business correspondence relating to a business relationship or an occasional transaction.

2) Records must be kept for five years from the date on which an occasional transaction is completed, or the business relationship ends, or in the case of transaction records, five years from when the transaction is completed and for all other records, five years from the date on which the business relationship end, unless the Commission specifies a longer period.

3) Records should be kept by way of original documents, by way of copies of original documents, certified where appropriate, as computerized, or other electronic data, as scanned documents, or using a combination of the above.

Note: DNFBPs are required to periodically review the accessibility of, and condition of, paper and electronically retrievable records and consider the adequacy of the safekeeping of records, and periodically test procedures relating to the retrieval of records.

ENHANCED DUE DILIGENCE

(Regulations 13 of the AML/PTF Regulations, Regulations 13 and 24 of the AML/PTF Code)

Describe in the AML Manual how the registrant will comply with enhanced due diligence requirements including:

i) What enhanced due diligence measures will be applied to:

- Non-face-to-face business?
- Persons or transactions involving a country identified as higher risk through the FATF?
- Persons or transactions involving higher risk countries for ML, TF, PF, and corruption or subject to international sanctions?
- Any other situation representing a higher risk of ML/TF/PF including those that you have identified in your risk assessment?

KEY POINT 1

The AML Manual must also set out what additional measures will be taken where enhanced due diligence is required to mitigate higher risk situations. At a minimum, the following measures must be taken:

1) Additional identification information must be obtained which should include the customer's identity, government issued identity number or other government identifier

2) Source of wealth of customer

3) Where a DNFBP is required by the AML/PTF Regulations to apply enhanced due diligence measures and undertake enhanced ongoing monitoring, the DNFBP must determine, based on the particular circumstances, what "specific and adequate measures" will be required to compensate for the higher money laundering and terrorist financing risks. These measures are almost certain to include obtaining further identification information and relationship information, including further information on the source of funds and the source of wealth.

POLITICALLY EXPOSED PERSONS

(Regulation 6 of the AML/PTF Regulations, Regulation 13 of the AML/PTF Code)

Describe in the AML Manual how the registrant will comply with enhanced due diligence requirements for politically exposed persons, including:

ii) A definition of what is a politically exposed person.

iii) How a politically exposed persons will be identified?

iv) What is the required approval(s) to do business with a politically exposed person?

v) How and what measures will be taken to establish source of wealth and source of funds?

vi) How will ongoing monitoring be conduct?

KEY POINT 1

The AML Manual must set out what additional measures will be taken where enhanced due diligence is required to mitigate higher risk situations. At a minimum, the following measures must be taken:

1) Additional identification information must be obtained, which should include the customer's identity, government issued identity number or other government identifier

2) Ascertain and document the source of wealth of the customer

3) Where a DNFBP i required by the AML/PTF Regulations to apply enhanced due diligence measures and undertake enhanced ongoing monitoring, the DNFBP must determine, based on the particular circumstances, what "specific and adequate measures" will be required to compensate for the higher money laundering and terrorist financing risks. These measures are almost certain to include obtaining further identification information and relationship information, including further information on the source of funds and the source of wealth.

ONGOING MONITORING

(Regulations 5, 11 and 13 of the AML/PTF Regulations, Regulation 28 of the AML/PTF Code)

Describe in the AML Manual how the registrant will comply with ongoing monitoring requirements including:

i) How will ongoing monitoring be conducted for:
- Business relationships
- Complex and unusual transactions

- Unusual patterns of transactions or activities which have no economic or lawful purpose

ii) How will the findings be recorded?

KEY POINT	
Examples of reports that enable ongoing monitoring and can be referenced in your AML Manual	
Key Topics to be Reported on	**Examples of Information to be Included in the Report**
Daily currency transaction	Payments made with cash
Large payments	Payments valued above an established threshold e.g. $10,000
Regulatory environment Results of internal testing Regulatory examination results	• AML/CFT regulatory changes • Internal audit testing results • Regulatory examination results • Remediation action plan and progress reports
Risk assessment	Potential changes in DNFBP's risk profile, including additional products and services, new higher-risk customers, and potential higher-risk geographies
High-risk customers (HRCs) and transactions	• New HRCs onboarded for the month • Total number of HRCs • Percentage of HRCs against customer base • Breakdown of HRCs by customer type (for example, PEPs, casinos) • Comparison of number of HRCs with that of previous month • Transactions that are sent to or received from a high-risk country or region • Payments that are sent to or received from a person or organisation on a sanctions list
Suspicious activity reports (SARs)	• SARs filing trends, number and percentage change of SARs filed in the last three months and prior year • Number of SARs filed after the 24 hours deadline for filing • Number of investigations in process versus number of investigations completed on a weekly basis for past three months • Number of investigations not yet completed in prior week for the past three months
Transaction monitoring alerts	• Number of alerts and investigations in the current queue this month (for example, number of open and closed alerts and investigations) • Number of alerts and investigations generated and closed last month • Number of alerts and investigations generated and closed in the prior three months

	• Identify the differences each month from generated and closed to the number of overdue alerts and investigations (for example, backlogs)
Customers with outstanding EDD/ CDD/identification verifications	• Number of new customers and number of identification verifications completed • Scheduled number of EDD requiring updating and number of EDD refreshes completed • Scheduled number of CDD requiring updating and number of CDD refreshes completed • Total number of outstanding EDDs/CDDs requiring completion • Percentage of HRC with incomplete EDD
Other compliance matters	• Training schedule and completion ratio • Staffing levels versus staffing plan • Key leadership/staffing shortages in critical compliance and operations departments

SUSPICIOUS ACTIVITY REPORTING

(Regulation 29 of the AML/PTF Code)

Describe how the registrant will comply with suspicious activity reporting requirements, including:

1) Defining what is a suspicious activity?

2) How the registrant (employees/agents) will identify suspicious activities (should refer to ML/TF indicators)

3) Who is the Money Laundering Reporting Officer (MLRO)?

4) Indicate the procedures for employees/agents to raise suspicions to the MLRO?

5) Specify that SARs filed with the FIA are confidential.

KEY POINT

The AML Manual must establish internal reporting procedures that provide that—

(a) where a customer fails to supply adequate customer due diligence information, or adequate documentation verifying identity (including the identity of any beneficial owners), consideration should be given to making a suspicious activity report;

(b) the reporting of all suspicious transactions, include attempted transactions, regardless of the amount of the transaction and business that has been refused;

(c) employees make internal suspicious activity reports containing all relevant information in writing to the MLRO as soon as it is reasonably practicable and, in any event, within twenty-four hours after the information comes to their attention;

(d) require suspicious activity reports to include as full a statement as possible of the information giving rise to knowledge or reasonable grounds for suspicion of money laundering or terrorist financing activity and full details of the customer;

(e) suspicious activity reports are not filtered out by supervisory staff or managers so that they do not reach the MLRO;

(f) suspicious activity reports be acknowledged by the MLRO.

The AML Manual should contain provisions for disciplining any employee who fails, without reasonable excuse, to make an internal suspicious activity report where he or she has knowledge or reasonable grounds for suspicion of money laundering or terrorist financing.

STAFF VETTING AND TRAINING

(Regulations 20 of the AML/PTF Regulations, Regulation 33 of the AML/PTF Code)

Describe how the registrant will comply with training requirements, including:

1) How will the registrant screen employees to ensure their competence and probity before hiring?

KEY POINT

Examples of steps that can be taken include:

(a) Obtaining identification information and verifying identity

(b) obtaining and confirming references with respect to prospective new employees;

(c) confirming the employment history and qualifications of prospective new employees;

(d) requesting and verifying details of any regulatory action taken against the employee concerned;

(e) requesting and verifying details of any criminal convictions.

2) How employees will be trained on:

- How to identify a suspicious transaction?
- What are the DNFBP's AML/PTF obligations?
- How to implement the registrant's policies and procedures?

KEY POINT

The AML Manual must include what measures the DNFBP have in place to make employees aware of:

(a) the AML/PTF procedures, systems, and controls in place to prevent and detect money laundering and terrorist financing;

(b)	employees' potential personal liability (criminal, regulatory and disciplinary) for breaches of the statutory provisions, and in particular for any failure to make a disclosure as required by section 127 of POCO;
(c)	potential implications to the DNFBP for any breaches of POCO, the AML/PTF Regulations and any applicable Code.