Frequently Asked Questions for DNFBPs supervised by The Compliance Commission of The Bahamas

The Compliance Commission of the Bahamas is issuing responses to frequently asked questions (FAQs) regarding Key Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) obligations, enforcement and customer due diligence requirements. These FAQs clarify the regulatory requirements to assist registrants with their compliance obligations in these areas.

Part 1
Key Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Obligations

Q. Who are Designated Non-Financial Business and Professions (DNFBPs)?

A. DNFBPs are also known as gatekeepers. They include: Lawyers, Accountants, Real Estate Brokers and Land Developers, Dealers in Precious Metals, Precious Stones and Pawn Brokers, and Persons Acting in the Capacity of a Trustee.

Q. Why should a DNFBP register with the Compliance Commission?

A. Section 33 of the Financial Transactions Reporting Act 2018 (FTRA 2018) makes it mandatory for every financial institution within the definition of section 32(2) to register with the Compliance Commission (CC). Businesses are required to register within one month of the coming into force of the FTRA 2018 and thereafter within one month of the commencement of the business. A DNFBP commits an offence and is liable to a penalty of five thousand dollars ($5,000) for each day that financial institution remains unregistered (refer to the CC's website under the Registration Tab, https://ccb.finance.gov.bs/registration/registration-requirements/).

Q. What is the purpose of the on-site and off-site examinations?

A. The purpose of these examinations are to assess the level of compliance of financial institutions with the requirements of Bahamian AML/CFT laws, obligations and guidelines.

Q. What is the frequency of the on-site and off-site examinations?

A. The Commission's frequency and intensity of the on-site and off-site examination of the DNFBP is on a risk sensitive basis, taking into account the risk rating assigned to the firm by the Commission, the risk rating score of the last on-site examination conducted, the Commission's understanding of the ML/TF risks profile of the firm, its characteristics and in particular its diversity, the identified ML/TF risks, the policies, procedures and internal controls associated with the DNFBP as identified by the Commission's assessment of the firm's risk profile and the ML/TF risks present in The Bahamas.

Q. Who conducts the examinantions?

A. A licensed public accountant conducts the routine on-site examination, who must first undergo the relevant training by the Commission prior to obtaining a Letter of Appointment, which gives him or her the authorization to commence an examination. A DNFBP may select the licensed public accountant of its choice, however, the examining accountant must be independent of the firm and the firm should satisfy itself that the examiner has a current and valid Letter of Appointment. The off-site examination of the firm will only be carried out by the Commission's Inspection Unit during a follow-up of a routine examination or during a risk assessment of the firm. The Commission staff may also conduct the routine on-site examination.

Q. What is an AML/CFT policies and procedures document?

A. An AML/CFT policy and procedure document is a written document that contains obligations applicable to the relevant business under the AML/CFT legislation and associated regulations and the corresponding processes and controls the firm has in place including when stated obligations are triggered, which sets out the DNFBP procedures for dealing with customers and the steps its staff have to undertake to mitigate risk to the firm. It should be approved by senior management, accessible to relevant staff and the supervisory authority and kept up-to-date.

Q. What is a documented ML/TF and other identified risk assessment and what should the DNFBP do?

A. A ML/TF and other identified risk assessment is a business-related risk assessment of a DNFBP risks. To execute a risk assessment the DNFBP must identify and assess the ML/TF risks related to customers, countries or geographic areas, products, services, transactions and delivery channels. Then adopt appropriate measures to mitigate the risk and efficiently allocate resources on higher risk identified i.e. controls, policies and procedures. The risk assessment must be appropriate to the size and characteristics of the DNFBP and approved by senior management. Within this framework "inherent risk" represents the exposure to ML/TF risks in the absence of any control environment and "residual risk" is the risk remaining after the appropriate control measures have been applied to the inherent risk. The residual risk should be within the DNFBPs risk appetite. The risk assessment must be reviewed and updated when there is any material change to the business, for example introduction of new products and services, as awareness of new vulnerabilities and typologies become known, important changes in existing products and services

and when new information on ML/TF typologies and national risks is available. Monitoring should be on-going as the risks may change significantly at any time and to the extent that the mitigation strategies become ineffective and require revision. The firm should establish an appropriate and continuing process for monitoring the risk, in particular, those activities assessed to be of a higher risk of ML/TF. The risk assessment must also be tested as part of the internal compliance effectiveness review obligation in the CC Codes, minimum every two years. The risk assessment is evaluated during on-site and off-site examinations.

Q. What is a facility holder?

A. A facility holder is the individual(s), company or partnership who the DNFBP is offering service to, it is the same as an account holder.

Q. Should a DNFBP have a Money Laundering Reporting Officer (MLRO)?

A. It is required by law under Regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations 2001 (FITRR 2001) and the MLRO must register with the Financial Intelligence Unit (FIU) and inform the Commission.

Q. Do we need to have a Compliance Officer (CO)?

A. Yes this is required by law under Regulation 5 of the FITRR 2001. According to the size of the firm one individual can hold both positions. However the CO does not have to register with the FIU but has to notify the Compliance Commission.

Q. What is an Eligible Introducer or third party introduction?

A. A third party/eligible introducer is any one listed under sections 3 and 4 of the FTRA 2018 or any foreign financial institution from a reputable jurisdiction who themselves are supervised or monitored for AML that is regulated by a body having equivalent regulatory and supervisory responsibilities as The Bahamas Regulators or any other foreign financial institution from a jurisdiction outside of The Bahamas as having an equivalent or higher AML regulatory framework to that which exists under Bahamian law. DNFBPs relying on a third party (domestically or within a foreign jurisdiction) shall immediately obtain all necessary information and documentation required under section 6(3) of the FTRA 2018 from the third party, including the identity of each facility holder and beneficial owner. Firms are also required to take adequate steps to ensure that the third party will upon request, provide copies of all relevant documentation without delay and is subject to AML obligations and is under supervision for compliance of these obligations. The company remains responsible for CDD obligations when they rely on another firm to carry out KYC requirements.

Q. Does the firm have to maintain transactions record and for how long?

A. Yes all DNFBPs must maintain transaction record keeping procedures as required by section 15 of the FTRA 2018. They must be kept for a period of not less than 5 years (refer to section 15 (2), FTRA 2018).

Q. What type of staff training a firm has to undertake and why?

A. All DNFBPs must receive AML/CFT/PF training. It should be done on an annual basis at a minimum as required by law under Regulation 6 of the FITRR 2001. It must be a part of the firm's written AML/CFT program (documented) and kept up-to-date.

Q. Why does my firm have to conduct an internal compliance effectiveness review?

A. DNFBPs are required to perform and document an internal compliance effectiveness review (every two years at a minimum) the results of which should be accessible for review both by examining independent accountants and the Commission's Examiners. The purpose of the effectiveness review is to assess the effectiveness of the firm's compliance program. The effectiveness review must cover and test all obligations applicable to your compliance program.

Q. What is a risk management system for customers and beneficial owners?

A. It is a risk system that is designed to screen clients to determine and monitor if they are PEPs or high risk clients or from higher risk country or jurisdiction. Further whether they are listed on the United Nations Sanctions list. They can be individuals or entities. They may also be subject to sanctions from any other official body or government that would prohibit the establishment of a facility or conduct of a transaction including attempted transactions. In addition to determine if they originate from a higher risk country as defined by Financial Action Task Force (FATF) and apply the appropriate measures.

Q. What is my firm's obligations under sections 43-49 of the Anti- Terrorism Act, 2018?

A. To be aware of and apply policies and procedures to implement the United Nations Security Council Resolutions including reporting to the FIU and Attorney General any assets frozen or actions taken in compliance with the prohibition requirements for Targeted Financial Sanctions related to terrorism/terrorist financing and proliferation financing, including attempted transactions.

Q. What is a list of individuals or designated entities distributed by the Compliance Commission and what must a firm do?

A. It is a list that is issued by the United Nations of individuals or designated entities regarding UN sanction Orders and firms are to search their clients data base and if there is someone they offer service to as a client, the firm must without delay freeze all the funds held by it in the name

of a designated entity and inform the FIU and the Attorney General as defined by law. Inform the designated entity that the funds have been frozen. Further, the firm must notify all "Hits or Nils" to the Commission.

Q. What happens to the frozen funds/assets?

A. (1) The designated entity may commence proceedings in the Supreme Court for an Order to release the funds fourteen (14) days after you have informed the designated entity that the funds have been frozen.

(2) The Attorney General may commence proceedings for an Order by the Court for the confiscation of the funds/assets held at any time after 14 days after the designated entity has been informed that the funds are frozen.

Part 2
Enforcement

Q. What is the Compliance Commission's authority to issue a penalty?

A. The CC has authority to issue a penalty under section 57 of the FTRA, 2018.

Q. What is an Administrative Penalty?

A. An Administrative Penalty is a monetary penalty imposed by the CC for non-compliance. Administrative Penalties provide an alternative reprimand and are imposed as a mechanism to enforce compliance with regulatory legislation and dissuade financial institutions and individuals from breaching their obligations under the FTRA 2018 or the Proceeds of Crime Act 2018.

Q. What type of violations will result in an Administrative Penalty?

A. The CC's Schedule of Offences are set out in the Codes of Practice issued to DNFBPs and can be found on the CC's website (refer to the CC's administrative penalty regime https://ccb.finance.gov.bs/wp-content/uploads/2020/04/Notice-Policyonadministrative penaltiesforconstituentsoftheCC Bahamas.pdf).

Q. What type of penalties will result from an Administrative Penalty?

A. Monetary

Q. What is the range of potential penalties?

A. A DNFBP can pay up to $200,000 while an individual can pay up to $50,000.

Q. How are notices regarding an Administrative Penalty issued?

A. Prior to implementing an Administrative Penalty, the Commission will issue a written warning via hand and email containing the nature of breach, the amount of the penalty if not remedied and a 28-day period to remedy the breach.

Q. What happens when a notice regarding an Administrative Penalty is issued?

A. After the notice is issued, you will have 28-days to remedy the breach acknowledged in the warning letter.

Q. What happens if I do nothing and ignore the Penalty Notice?

A. If the 28-day period expires and the breach is not remedied, a letter allowing for an additional 48-hour period to remedy the breach is issued. Failure to comply after this letter is issued will lead to a letter advising of the amount of money owed to satisfy the penalty.

Q. How long do I have to pay the fine?

A. Seven days.

Q. What happens once I remedy the breach and pay the fine?

A. Once the breach is remedied, the Commission will issue a letter to acknowledge the resolution and a receipt to acknowledge the payment of the fine.

Q. How can I avoid a penalty?

A. Comply with the directives of the Commission, the Codes of Practice and relevant legislation.

Q. I have failed to comply previously, why am I now receiving a penalty?

A. The Commission's Policy on Administrative Penalties came into effect on February 6th, 2019. The Policy was not available for any non-compliance prior to.

Q. Why wasn't I informed about this new Policy?

A. The Commission issued the Policy via email to its registrants upon the enactment of the Policy (refer to the CC's administrative penalty regime - https://ccb.finance.gov.bs/wp-content/uploads/2020/04/Notice-PolicyonadministrativepenaltiesforconstituentsoftheCC Bahamas.pdf).

Q. What happens if I fail to report to the Financial Intelligence Unit that I hold funds/assets for a designated entity?

A. You have committed an offence and are liable on summary conviction to a fine not exceeding two hundred and fifty thousand dollars. Refer to section 49 of the Anti-Terrorism Act, 2018.

Part 3
Customer Due Diligence

Q. What Is Customer Due Diligence (CDD)?

A. Customer Due Diligence (CDD) also referred to as know your customer (KYC) is a process that DNFBPs use to determine the identity of potential clients and assesses the level of risk they possess. The risk assessment enables the DNFBP to measure the extent to which the customer exposes it to a range of risks. These risks include money laundering (ML) and terrorist financing (TF).

Q. When Is CDD Carried Out?

A. DNFBPs normally carry out CDD measures in the following circumstances:

(i) **New business relationship:** DNFBPs typically perform due diligence measures prior to establishing a business relationship.

(ii) **Occasional transactions:** Certain occasional transactions warrant CDD measures, these could involve amounts of money over a certain threshold.

(iii) **A "trigger" event occurs:** when a trigger event occurs e.g. suspicions of ML concerns are raised regarding previous information collected and its' validity or the product/service offered to the customer changes.

Q. Is CDD Required by Law?

A. Yes CDD is required by Law in the Bahamas. Section 6 of the Financial Transactions Reporting Act 2018 stipulates "every financial institution shall undertake customer due diligence measures when opening an account for or otherwise establishing a business relationship with a facility holder……." (refer to Sections 6-14 of the FTRA 2018).

Q. What Is a CDD/KYC Form?

A. CDD/KYC form is a document that a DNFBP creates for gathering personal information on the client or potential client during the onboarding process. It is usually in the form of a checklist to verify that the DNFBP has collected all of the required information and documents.

Q. What is CDD Information Used for?

A. By obtaining relevant personal CDD information e.g., name, address, phone, date of birth, source of funds, copy of passport or photo ID, this information is typically used to: (1) identify and verify the customer and their activities, (2) monitor customer's transactions, (3) Identify the Beneficial Ownership (BO) & control structure of company structures and (4) assist law enforcement by providing available information on customers or activities and transactions being investigated.

Q. Why Is CDD Important?

A. CDD is vital because it protects the DNFBP from dealing with customers involved in illegal or questionable activity. CDD similarly aids in determining the new customers **risk level** of engaging in future financial crimes. By performing CDD, the DNFBP is able to differentiate between higher and lower-risk customers through its risk- assessment process. Through CDD processes the DNFBP is also able to provide more scrutiny of higher risk customers by clearly defining the risk mitigation measures to be applied.

Q. What are the Risks of not Carrying out CDD?

A. Without performing CDD, the DNFBP risks harming its reputation if the customers business is involved in money laundering, terrorist financing, & corruption. The DNFBP could also become the target of legal or regulatory actions, it may suffer financial loss and also risk receiving administrate penalties/fines imposed by the Compliance Commission (CC). Additionally, an effective CDD Program will also assist in protecting the financial sector as a whole from the threats of ML/TF and other identified risks, which can result in reputational damage for the country.

Q. What is The Risk Based Approach to CDD?

A. The Risk Based Approach (RBA) to performing CDD, means that the CDD process is **risk** sensitive and the DNFBP applies the appropriate measures, checks, and controls **proportionate** with the level of risk posed by the potential customer. When applying the RBA, DNFBPs are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

Q. What Is Enhanced Customer Due Diligence (ECDD)?

A. ECDD, which is a higher level of due diligence is required where the customer and product/service combination is considered to be a greater risk. This higher level of CDD is required to mitigate the increased risk. Some **ECDD measures** involve: (1) making additional checks on a **customer's** identification, (2) collecting extra information and carrying out additional verification and (3) confirmation of source of funds or an adverse media check. Enhanced measures shall always be effective and proportionate to the risk identified.

Q. What are Some Characteristics of Higher Risk Customers in ECDD?

A. Some characteristics include:

(i) Client or Beneficial Owner is or has links to a politically exposed person (PEP), terrorists, criminals or an individual or entity on a sanctioned list.
(ii) Client comes or operates from a jurisdiction considered to be high risk.
(iii) Client is involved in a Cash intensive business.
(iv) Non face to face business relationship and interactions with clients.
(v) Questionable source of assets or funds.

Q. What Is Standard Customer Due Diligence?

A. Standard Customer Due Diligence is carried out generally in situations where there is a potential risk, but it is unlikely that the risks will be realized. Standard due diligence requires the DNFBP to identify the customer as well as **verify** their identity. There is also a requirement to gather information to get an understanding of the nature of the business relationship and to monitor the client and the relationship, this will highlight any potential trigger events that may result in further due diligence being required. An **example** of a standard risk customers is one who is permanently resident in the country, with a salaried job or other transparent source of income.

Q. What Is Simplified Due Diligence?

A. Simplified due diligence (SDD) is the lowest level of due diligence that can be completed on a customer. SDD is the opposite of enhanced due diligence or a **less** rigorous version of standard due diligence and is appropriate where there is little opportunity or risk of the DNFBPs services or clients becoming involved in money laundering or terrorist financing. With SDD, there is no requirement to **verify** your client's identity. Example (i) public companies listed on a stock exchange and subject to disclosure requirements and (ii) public administrations or enterprises.

Q. What Is Ongoing Customer Due Diligence?

A. Ongoing customer due diligence (OCDD) is the process of revisiting and re-verifying the information gathered during CDD. OCDD involves the continued **monitoring** of the DNFBPs business relationships and includes the scrutiny of transactions undertaken throughout the course of the relationship. This scrutiny ensures that transactions being conducted are consistent with the DNFBPs knowledge of the client, their business and risk profile, including, where necessary, the source of funds. OCDD helps to identify patterns that may increase a clients' risk profile & involves: (i) Monitoring transactions to confirm legitimacy; (ii) observing business activities to ensure they match the client profile as stated during CDD, (iii) reviewing the information provided during the CDD process regularly for changes or inconsistencies with client profile and (iv) keeping relevant data and documents updated for future reference.

Q. Does CDD require the Verification of Beneficial Owner (BO)?

A. DNFBPs are required by law to identify and verify the beneficial owner of a facility, if any, and where the facility holder is a corporate entity, the obligation to verify the identity of beneficial owners will only be required for those beneficial owners having a controlling interest of 10% or greater in the corporate entity. Where no natural person is identified, the identity of the relevant natural person who holds the position of Senior Managing Official is verified (refer to regulation 5(1)(e), FTRR 2018 and regulation 10, FTRR 2018).

Q. What are Benefits of Customer Due Diligence?

A. The benefits of CDD include:

(i) Compliance with safe DNFBP international best practices, such as those established by the Financial Action Task Force (FATF), and legislative and regulatory requirements,
(ii) Understanding the customer's risk profile and assessing their risk level before the account is open,
(iii) Mitigate the risk identified in the risk assessment,
(iv) Ability to focus more attention and resources on high-risk customers,
(v) Easier prediction of activities the customer is likely to engage in (and identification of unusual or illegal activity during the course of the business relationship), and
(vi) Enabling the business to assist law enforcement when needed.

Q. When Performing CDD is Anyone Exempt from Verification?

A. Documentary evidence will **not** normally be required for verification of identity of:

(a) Any financial institution licensed by the Central Bank of The Bahamas, The Securities Commission of The Bahamas, The Inspector, Financial Corporate Service Providers, The Insurance Commission of The Bahamas, or the Gaming Board;
(b) A financial institution which –
  (i) Is subject to anti-money laundering and countering the financing of terrorism obligations;
  (ii) is under supervision for compliance with the obligations referred to in subparagraph (i); and
  (iii) has adequate procedures for compliance with customer due diligence and record keeping requirements;
(c) Any central or local government agency or statutory body; and
(d) A publicly traded company listed on The Bahamas International Stock Exchange or any other Stock specified in the Schedule and approved by the Securities Commission of The Bahamas (see regulation 8, FTRR 2018 and the Schedule therein).

For more information regarding questions you may have, please contact us at: **compliance@bahamas.gov.bs** and the CC website for relevant AML/CFT legislation, Codes and guidance.

Issue Date: 23rd October, 2020.

The Compliance Commission
#31 Poinciana House
East Bay Street
P.O. Box N-3017
Nassau, Bahamas
Telephone: (242) 604-4331
Email: Compliance@bahamas.gov.bs
Website: https://ccb.finance.gov.bs