MONEY LAUNDERING & THE FINANCING OF TERRORISM

GUIDELINES FOR FINANCIAL INSTITUTIONS

Update

Published: 27 October 2022

The Supervisory Authority and
Director of the ONDCP
ONDCP Headquarters
Camp Blizard
Antigua and Barbuda
Telephone: 562-3255, (268) 462-5934
Fax: (268) 460-8818
Email: supervisory.authority@ondcp.gov.ag

NOTICE

To All Financial Institutions:

TAKE NOTICE that the Money Laundering & the Financing of Terrorism Guidelines for Financial Institutions are hereby amended by the update annexed hereto pursuant to the powers of the Supervisory Authority under sections 11(1)(c) of the Money Laundering (Prevention) Act 1996 [as amended by section 7 of the Money Laundering (Prevention) Act 2018].[1]

Issues addressed:

- outsourcing of the compliance function;
- clarification of procedures for verification of customer identity;
- correction of an inadvertent typographical error in the guidance with respect to CDD relating to insurance;
- new guidance in relation to production orders and directives.

27 October 2022

Lt. Col. Edward Croft
Director of the ONDCP and
Supervisory Authority under the
Money Laundering (Prevention) Act 1996

[1] Financial institutions have 14 days from the date of publication in which to raise with the Director of the ONDCP in writing any concerns about the amendments or any other issue prompted by this guidance that relates to their ability to effectively follow the guidance.

ANNEX

UPDATE of the Money Laundering & Financing of Terrorism Guidelines

26 October 2022

The Money Laundering & the Financing of Terrorism Guidelines for Financial Institutions (abbreviated herein as "MLFTG") are hereby amended as follows:

A. In Part I - Money Laundering of the MLFTG

(a) Section 1.1A is repealed and substituted with the following:

"Outsourcing of the Compliance Function

1.1A (1) The compliance function of financial institutions can be contracted out, that is, outsourced to a person with sufficient expertise. However, in doing so, a financial institution does not outsource its legal liability for that function and remains responsible for everything the contractor does in carrying out the function, including mistakes, errors and negligence.

(2) Where the compliance function is outsourced, the person to which it is outsourced *does not* become the financial institution's Compliance Officer, as that function must remain with the inhouse Officer legally responsible for carrying out the functions under para. 1.1.

(3) A financial institution is responsible for systems and controls operated by the outsourced contractor in carrying out any part of the compliance function.

Actions required to be taken

(4) Where a financial institution outsources all or part of its compliance function, it must maintain appropriate control and oversight over the outsourced activity [see also Part II – Terrorism Financing, para 1.2].

(5) A financial institution must ensure that the business performing an outsourced compliance function:

(a) has sufficient of the financial institution's relevant information to enable it to make necessary determinations, particularly in respect of detecting suspicious activity and preparing SARs;

(b) has access to relevant records, background information, history and previous transactions records of the financial institution;

(c) has adequate resources to carry out the compliance function outsourced to it.

(6) Where there is no access to information under (5), the person performing the sourced compliance function is unlikely to be in a position to adequately fulfill its function competently or

adequately.

(7) Suspicious Activity Reports are required to be filed by the Compliance Officer (see para. 1.1(2)), which means that it is to be filed by the inhouse officer with legal responsibility for making such filings. SARs should therefore not be filed by a person responsible for performing an outsourced compliance function. Instead, SARs prepared by this person should be submitted for review and filing to the Compliance Officer.

(8) Where the person performing the outsourced compliance function is authorized by the financial institution to submit on its behalf any information (other than a SAR) to the Supervisory Authority or Director of the ONDCP, the person in doing so, must furnish the Compliance Officer with a copy of the information or communication.

1.1B Financial institutions should put in place adequate screening procedures to ensure high standards when hiring employees. This can include obtaining proper documents of identification, references, and where appropriate police records and assessments from past employers.

(b) under the heading "WHEN IDENTITY MUST BE VERIFIED", Sections 2.1.9 and 2.1.10 of the MLFTG are repealed and substituted with the following:

"2.1.9 Whenever a business relationship is to be established, e.g. when an account is opened with the financial institution, or a significant one-off transaction or series of linked transactions are undertaken, the customer must produce evidence of his/her identity and the identity must be verified by the financial institution.

2.1.10 (1) Once verification of identity procedures have been satisfactorily completed and a business relationship established, no further **verification of identity** is required for subsequent transactions by the customer. However, ongoing customer due diligence as called for by regulation 4(3)(l) of the MLPR and defined in regulation 2, may in some circumstances, create the need for re-verification of identity as discussed below in paras. (2) and (4).

(2) In updating or maintaining customer account records, financial institutions are expected to apply on-going *know your customer* procedures in order to monitor and stay current with the affairs and activities of the customer. Ongoing customer due diligence emphasizes monitoring of the relationship to ensure "that the transactions being conducted are consistent

with the financial institution's knowledge of the customer, the business and risk profile and keeping the information up to date and relevant, especially for high risk customers and PEPs. An example of this would be when an ordinary customer becomes a PEP or an ordinary customer is publicly referred to as being connected with criminal activity such as but not restricted to drug trafficking.

(3) During the lifetime of the business relations, a financial institution should ensure that customer profiles are current and reflective of the customer's financial status, source of funds and source of wealth. Financial institutions should ensure that there is consistency in the purpose and use of the business relationship. These aspects of customer profiles should remain current and all changes should be verified with supporting documentation.

(4) Any significant change in these activities, the nature or scale of the customer's business or transactions being carried out will affect the customer's risk profile and should be reported to the Compliance Officer, who if he/she deems it necessary or appropriate in accord with the Risk Management policy and procedures of the financial institution, should update the customer's risk profile and where necessary report it to senior management. For example, a customer who opens an account as an unemployed college student should not years later when he has become the CEO of a company, have the same profile or account details even though his identity is not in question."

(5) When an existing customer closes one account and/or opens another there is no need to re-verify the customer's identity once the business relationship has not become inactive (no transactions for a year or more)..

(6) Where a business relationship becomes inactive (no transactions for a year or more) a customer's identity should be re-verified in the event that the customer wishes to recommence business activity.

(7) Where at any time after verification of identity has been completed the financial institution (particularly its customer service officer or any employee responsible for creating, amending or maintaining customer account records), has reason to *doubt the veracity or accuracy* of the information contained in the record of identity of a customer, then that person should bring this to the Compliance Officer's attention,

and the Compliance Officer must determine if in the circumstances there is doubt sufficient to warrant the re-verification of the customer's identity. This situation would not include the mere fact that an established customer seeks to open a new personal or business account."

(c) Under section 2.1.14A(3) of the MLFTG, paragraph (a)(2) is repealed and substituted with the following:

"(2) Financial institutions should include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. This should include determining if the beneficiary is a PEP, and where the beneficiary has a beneficial owner then determining if the beneficial owner is a PEP."

(d) Section 2.1.39 of the MLFTG relating to incorporated entities is amended at para. (e), by replacing the full stop with a semi-colon and inserting the following bullet point:

"(f) certificate of good standing."

(e) Section 2.1.39B of the MLFTG relating to unincorporated businesses and partnerships is amended by inserting after the last bullet point, the following:

"• certification of current registration."

(f) After section 4.15 of the MLFTG under the heading "INTERNAL REPORTING PROCEDURES AND RECORDS" there is inserted the following heading and sections:

"On Becoming Aware of a Criminal Investigation

"4.15A (1) There are a number of ways in which a financial institution might acquire knowledge of or have reason to suspect a customer is the subject of or associated with the subject of a criminal investigation relating to money laundering or other financial crimes that are the predicates to money laundering. Statements in the press or public allegations, complaints or bringing of charges are obvious sources. However, sometimes, compelling instances are those where a financial institution is served with a Production Order by law enforcement or receives a Directive from the ONDCP requesting information.

(2) In the case of a Production Order, the financial institution and the Compliance Officer in particular should bear in mind that in order for the Court to grant a production order, the conditions in section 15 of the MLPA have to be satisfied: That is that a judge of the High Court must be persuaded that there are

reasonable grounds for believing that a person, the subject of the order, is committing, has committed or is about to commit a money laundering offence or has engaged or is about to engage in money laundering activity. Alternatively, under section 42 of the POCA, that there are reasonable grounds to believe that a person has committed a Schedule offence under the POCA.

(3) In the case of a Directive (informal request for information) to a financial institution relating to a customer made under section 11A(h) of the MLPA, the Directive is issued on the basis that the request is in support of an investigation of money laundering or the financing of terrorism.

(4) Therefore, Production Orders and Directives by their very nature tend to disclose a direct or indirect connection of a subject to a financial crime investigation.

(5) Financial institutions are expected not only to comply with the order or directive but also to take appropriate mitigating measures in light of the heightened risk exposure of the institution to a customer who may be directly or indirectly connected to a financial crime investigation. Such measures could include but need not be limited to: (a) Enhanced transaction monitoring of an existing customer who is the subject of a Production Order or Directive. This brings about increased focus on the degree to which transactions are consistent with the declared purpose for the opening of an account, the expected account activity, the current updated status and profile of the customer and his/her business relations. (b) Due diligence screening of new customers against databases of persons and entities that have been the subjects of production orders or directives prior to the new application to open a business relationship or conduct a one-off transaction. This allows the financial institution to be better able to identify at an early stage of the business relationship or one-off transaction customers who may pose a higher risk."

Supervisory Authority and
Director of the ONDCP