مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANISATIONS

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS PROVIDING SERVICES TO CASH-INTENSIVE BUSINESSES

September 27, 2021

Contents

1. Introduction

1.1 Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices, and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

1.2 Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and
- Insurance companies, agencies, and brokers.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.3 Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations ("AML-CFT Law").

- Cabinet Decision No. (10) of 2019 Concerning the Implementation Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations ("AML-CFT Decision").

1.4 Definitions

Bearer Negotiable Instruments: Financial instruments of whatever form, whether in the form of a bearer document, such as: traveler's cheques; promissory notes and cheques, payment orders, or others. These instruments may either be in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; or may be incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.

CBUAE Regulations: Any resolution, regulation, circular, rule, instruction, standard or notice issued by the Central Bank.

Cash Couriers: Natural persons who physically transport currency and bearer negotiable instruments on their person or accompanying luggage from one jurisdiction to another.

Cash or Currency: Banknotes and coins that are legal tender in circulation as a medium of exchange.

Cross-Border Transportation of Currency or Bearer Negotiable Instruments: Any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency through containerized cargo; or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.

Predicate Offense: Any act constituting a felony or misdemeanor under the applicable laws of the UAE whether this act is committed inside or outside the UAE when such act is punishable in both countries.

2. Understanding Risks

2.1 Vulnerabilities of Cash

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that, as the UAE is a cash-intensive economy and plays an important part in global trade, there are significant risks associated with the cross-border movement of cash and bearer negotiable instruments, including bulk-cash smuggling that is associated with third-party money laundering risks.

As a major medium of exchange in the UAE, cash is particularly vulnerable to abuse by illicit actors to conduct money laundering activities and finance criminal activities. The specific characteristics of cash—anonymity, interchangeability, and transportability—make it an attractive method by illicit actors seeking to conceal the proceeds of crime. Unlike other monetary instruments, such as credit cards or wire transfers, cash holds no record of its source or owner, and can be easily concealed in large quantities upon which it is difficult to trace once spent. Cash transactions are also instantaneous and widely accepted across jurisdictions.

Criminal activity—or a predicate offense—is often cash based. A predicate offense for money laundering is the underlying criminal activity that generates proceeds. Criminals then seek to "launder" these illicit proceeds, which leads to the offense of money laundering. The FATF Recommendations identify "designated categories of offenses"[2] as the following:

- Participation in an organized criminal group and racketeering;
- Terrorism, including financing of terrorism and illegal organisations;
- Trafficking in human beings and migrant smuggling;
- Sexual exploitation, including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint, and hostage-taking;
- Robbery or theft;
- Smuggling;
- Tax crimes;
- Extortion, Forgery;
- Piracy and
- Insider trading and market manipulation.

However, as the FATF expects countries to include the above-mentioned list at the minimum, the UAE's definition of Predicate Offense is broader to include **any act** constituting a felony or misdemeanor under the applicable laws of the UAE, whether this act is committed inside or outside the UAE when such act is punishable in both countries.

2.2 Vulnerabilities of Alternatives to Cash

Illicit actors also use various monetary instruments in conjunction with, or as a replacement to, cash. Both bearer negotiable instruments and prepaid cards for instance offer similar benefits to cash, including anonymity and accessibility. They can store large amounts of value in a compact physical size that makes

[2] Available at https://www.fatf-gafi.org/glossary/d-i/

them potentially vulnerable to abuse by illicit actors who use them instead of cash to make physical cross-border transportations of value. Illicit actors seeking to avoid an LFI's identification and verification requirements can exploit the ease of payment offered by bearer negotiable instruments and prepaid cards for the purpose of moving their proceeds—thus obscuring the origin of the funds—and converting them to payments for other goods or services. This may also include obtaining funds in one jurisdiction and having access to cash withdrawals in another jurisdiction. Additional characteristics and associated vulnerabilities of bearer negotiable instruments and prepaid cards are discussed below.

2.2.1 Bearer Negotiable Instruments

Bearer negotiable instruments are financial instruments of whatever form, whether in the form of a bearer document, such as traveler's cheques, promissory notes and cheques, payment orders, or other forms that can be attractive to illicit actors as alternatives to cash. Bearer negotiable instruments provide the opportunity to move large amounts of funds in bearer form without the bulkiness of cash. They are transferable documents that provide unconditional guarantees of cash payments either on demand or at a future date. The individual who issues a negotiable instrument is known as the 'payer' or 'issuer,' and the person who receives a negotiable instrument is known as the 'bearer' or 'payee'.

Bearer negotiable instruments often include the instruction 'pay to the bearer', meaning the bearer would be the person in physical possession of the instrument. The risk, in this scenario, is that the holder is a criminal and/or not the intended payee of the negotiable instrument. Bearer negotiable instruments are also unique in that they can also be easily transferred from one party to another, which effectively obscures the paper trail on the 'payer' or 'issuer', and enables illicit actors to distance the proceeds of crime from the illegitimate source. **LFIs should seek to mitigate these risks by continuing accepting cash and third party cheques as long as the due diligence measures regarding the person presenting the cheque have been duly conducted by the LFI.**

2.2.2 Prepaid Cards

Prepaid cards can be used as an alternative to cash in that they provide access to funds that have been paid in advance. Funds can be claimed or transferred through an electronic device, such as through a card, code, electronic serial number, mobile identification number, or personal identification number within either an "open" or "closed" loop system:

- "Open loop" prepaid cards can be used for purchases at any merchant where that brand of the card is accepted and offers access to cash at any automated teller machine ("ATM") that connects to the affiliated ATM network. Some prepaid cards may be reloaded, allowing the cardholder or third-party (such as an employer) to add value to the card. For example, a travel card can allow cardholders to top up at various locations, including online and at kiosks, and then allows cardholders to utilize the card to purchase local travel as well as goods or services at various participating stores.
- "Closed loop" prepaid cards generally can only be used to buy goods or services from the issuing merchant of the card or a select group of merchants that participate in that specific network. These cards generally do not allow for cash access, although they can often be re-sold through third-party websites in exchange for other closed loop cards or payments. For example, a chain of coffee shops may offer reloadable cards that can only be used to purchase goods at the coffee shop.

Prepaid cards can be abused by illicit actors seeking to launder money and finance terrorist activities. For instance, both open and closed loop prepaid cards can be utilized in conjunction with, or as a replacement to, bulk cash smuggling. Specifically, drug traffickers have been known to convert cash derived from narcotic sales to prepaid debit cards, which they then use to purchase goods and services or send to narcotic suppliers, who in turn use the cards to withdraw cash from an ATM. In addition, funds can be loaded onto prepaid cards in support of terrorist activities, such as purchasing various products and services whether buying a terrorist a plane ticket or providing other resources (e.g. car rental or hotel) to support a terrorist group.

When assessing the risks associated with prepaid cards, LFIs should consider the specific risks posed by the features and functionalities of the monetary instrument. If the cardholder is anonymous, or if the holder or purchaser provides false information on their identity for instance, the money laundering and financing of terrorism and illegal organisations risks are higher. In addition, LFIs should evaluate the risks associated with cash access, and the volume and velocity of funds that can be loaded and retrieved on prepaid cards. Further risk factors include type and frequency of loads and transactions, geographic location where the transaction activity occurs, value limits, distribution channels, and the nature of funding sources.

2.3 Vulnerabilities of Cash-Intensive Businesses

2.3.1 Types of Cash-Intensive Businesses

Cash-intensive businesses are businesses that experience a high volume of cash flows. However, because cash-based transactions are inherently difficult to trace, as discussed above, cash-intensive businesses may potentially be used as vehicles for money laundering and the financing of terrorism and illegal organisations. Businesses that generate a large volume of cash revenue may be susceptible to abuse by illicit actors that integrate the proceeds of crime into the banking system under the guise of legitimate business. In particular, they may exploit cash-intensive businesses for money laundering and the financing of terrorism and illegal organisations by using cash-intensive business to:

- Provide a front to launder large amounts of cash and reinvest cash proceeds of crime in the economy;
- Co-mingle illicit and legitimate income; and
- Finance, though often through small amounts of cash, terrorist activities without traceability.

Cash-intensive businesses span across various industry sectors. Most of these businesses are operating a legitimate business; however, some aspects of these businesses may be vulnerable to money laundering or the financing of terrorism and illegal organisations. Examples of cash-intensive businesses include but are not limited to the following:

- Convenience stores;
- Retail stores;
- Restaurants;
- Wholesale or general trading businesses;

- Travel agencies and tour operators; and
- Car dealers.

In addition, please consult the CBUAE's *Guidance for Licensed Financial Institutions providing services to the Real Estate and the Precious Metals and Stones sector* [3] for further information.

LFIs may expand on the above by considering additional factors when identifying cash-intensive businesses in their customer base. For example LFIs can define cash-intensive businesses based on specific criteria, such as a proportion or more of the business' revenue is in cash or the business has a monthly revenue in cash above a certain threshold. In either scenario, the definition of cash-intensive business should be determined by the LFI, justified by a sound methodology that considers various factors including risk and characteristics, documented in the LFI's policies and procedures, and approved by the LFI's senior management.

The LFI should monitor whether the cash-intensive business appears to generate unusual transactions compared to the business' expected activity and profile, and with other similar cash-intensive businesses. For example, a small business making significantly larger amounts of cash deposits than other businesses of a similar size in the same industry should be reviewed for potential money laundering activity. The extent of the vulnerability presented by cash-intensive businesses may be particularly severe due to large volumes of cash transactions, limited record keeping, and high customer turnover. LFIs should therefore understand the nature and purpose of the business relationship and expected activity of the customer in order to identify types of transactions that appear to be unusual, potentially suspicious, and/or inconsistent with the customer's profile and stated purpose of the account.

The following sections examine common features of cash-intensive businesses that impact risk. **LFIs should consider the specific risks posed by these features to determine whether the customer is considered as high-risk and should be subject to enhanced due diligence ("EDD") measures.** LFIs should incorporate this assessment into their AML/CFT program and update their policies, procedures, and processes with the aim to detect illicit activity and manage illicit financing risks.

2.3.1.1 Cross-Border Movement of Cash and Cash Couriers

Cash-intensive businesses may move cash across borders as part of their business model. Cross-border movement of licit cash can be legal, subject to compliance with reporting and other relevant legal and regulatory requirements. However, criminals may also seek to move cash across borders; according to FATF, the physical transportation of cash across an international border is "*one of the oldest and most basic forms of money laundering*" and is still widely used today.[4] The criminal economy tends to be cash-based with illicit proceeds of crime moving quickly and anonymously, including across borders. Illicit actors often choose to remove their illicit assets from a bank account in order to obscure the audit trail by transporting it to another country where they can spend the cash on goods or services or reintroduce the cash into the financial system. Illicit actors who generate cash proceeds also seek to move their profits to jurisdictions that will allow the placement of cash into the legal economy without detection. Their selection of a jurisdiction can be driven by the predominant use of cash in that jurisdiction, the weaker AML/CFT controls of a jurisdiction's financial system including few or no restrictions on cash payments, or a

[3] Available at https://www.centralbank.ae/en/cbuae-amlcft.
[4] FATF "Money Laundering through the Physical Transportation of Cash" (October 2015), available at: https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf

jurisdiction's reputation as a banking secrecy haven. Illicit actors can exploit the high volume of passenger, cargo, and mail movements into and out of jurisdictions to move cash without attracting the attention of authorities.

Cash-intensive businesses may utilize cash couriers to move cash across borders. Cash couriers are natural persons who physically transport currency and bearer negotiable instruments on their person or accompanying luggage from one jurisdiction to another. Couriers may be directly involved in the underlying crime or may be third parties recruited specifically to move money to another jurisdiction. Mechanisms to conceal the cash include within pieces of clothing on the physical persons (such as a money belt), hidden within luggage, or even concealed internally. Cash couriers may use air, sea, or rail transport to cross an international border and typically use high denomination banknotes as part of their transportation, which decreases the size and bulk of low denomination banknotes.

Specifically, cross-border movements of cash across an international border are used to:

- Launder proceeds of crime by placing them in another jurisdiction, typically with weaker AML/CFT controls.
- Move illicit value to purchase assets that can hold considerable value, such as luxury goods, or transfer the value of the funds for them to be stored.
- Hide proceeds from authorities and complicate asset recovery.

It is not illegal to move cash into or out of the UAE. However, natural or legal persons must declare upon entering or leaving the UAE any currencies, bearer negotiable instruments, precious metals and stones above the threshold of AED 60,000. The relevant extract of the Regulation on the Declaration of Currencies, Bearer Negotiable Instruments, and Precious Metals and Stones in Possession of Travelers Entering or Leaving the UAE (issued in the Official Gazette No 703 dated 31/05/2021) is in the box below.

Article (8) of Federal Decree-Law No. (20) of 2018 on Anti Money Laundering and Combating the Financing of Terrorism and the financing of Illegal Organizations stipulates that (when entering or leaving the country, any person must declare the currencies or bearer negotiable financial instruments, precious metals or stones of value, in accordance with the declaration regulation issued by the Central Bank).

Accordingly, the Board of Directors of the Central Bank has decided that the maximum threshold for currencies, bearer negotiable instruments, and precious metals and stones, shall be in accordance with the table below, and shall apply to all forms of physical cross-border transportation, whether by travelers or through mail and cargo. Bearer negotiable instruments mean financial instruments of whatever form, whether in the form of a bearer document, such as travelers checks, promissory checks, payment orders, or others. Based on the above, any natural or legal person shall declare upon entering or leaving the UAE any currencies, bearer negotiable instruments, precious metals and stones above the threshold specified in the table and shall provide an honest and clear answer and adequate information to the Customs authority and its staff upon request. Declarations shall also be made for currencies, bearer negotiable instruments, precious metals or stones of a value exceeding the specified threshold crossing the border through cargo, mail or shipments transported using transport service companies using the official customs systems of the UAE.

Maximum threshold for currencies, bearer negotiable instruments, and precious metals and stones	
Currencies/Instruments/Metals/ Precious stones	**Threshold above which declaration is required**
1. Currencies (UAE Dhrs or equivalent in other currencies)	UAE Dhrs 60,000 or equivalent in any other currencies
2. Any type of bearer negotiable instruments	UAE Dhrs 60,000 or equivalent in any other currencies
3. Precious metals with high economic value in any form, type or classification, provided they are not intended for commercial purposes or transported by a traveler that engages in the same trade or a traveler that transports such materials as a profession and frequently visits the department or the customs port.	UAE Dhrs 60,000 or equivalent in any other currencies
4. Precious stones with high economic value in any form, type or classification, provided they are not intended for commercial purposes or transported by a traveler that engages in the same trade or a traveler that transports such materials as a profession and frequently visits the department or the customs port.	UAE Dhrs 60,000 or equivalent in any other currencies

Understanding whether customers have made any such declarations, in accordance with the Regulation should form part of any due diligence by the LFIs where required. As part of due diligence, LFIs may require additional information on the customer or the transaction, including the source of funds and relevant documentation.

Potential Risk Indicators:

- Transactions involving locations or customers originating from locations with poor AML/CFT regimes or high exposure to corruption.
- Significant and/or frequent cash deposits or currency exchanges made over a short period of time.
- Customer is in possession of money supposedly for business reasons while travelling to countries where cash payments are restricted.
- Customer requests to purchase, or has possession of, large volumes of high denomination banknotes.
- Customer requests to purchase, or has possession of, large amounts of foreign currency without a plausible explanation.
- Customers who use false identification or offer different identifications on separate occasions

2.3.1.2 Cash Deposits

Cash-intensive businesses can be expected to make cash deposits, which is legal and a natural fit with their business model. Illicit actors, however, will seek ways to place their illicit cash into the financial system. Illicit actors involved in cash generating crimes frequently need to use a significant portion of the cash they have acquired to pay for the illicit goods they have sold, to purchase additional goods, and to pay the various expenses incurred in acquiring or transporting the goods. As part of the money laundering process, individuals seek to use the proceeds of crimes by disguising the origin of the funds as legitimate economic

activities. Terrorists also seek to finance, often through small amounts of cash, terrorist activities without traceability. LFIs should therefore be aware of cash deposits placed into the banking system that involve high-risk customers and/or geographical areas, third parties without a relationship to the customer, and transactions that lack an apparent business purpose. LFIs should, as the case may be, undertake CDD measures on the third party cash depositors transacting in any accounts above the threshold specified in Article 6 of the AML-CFT Decision. **LFIs should also obtain appropriate information regarding the source of cash deposited in a customer's account as well as mandate the use of Emirates ID for cash deposits in ATMs.**

- **Potential Risk Indicators:**
  - Large cash deposits followed immediately by withdrawals or electronic transfers.
  - Large cash deposit followed by an immediate request that the money be wired out or transferred to a third party, without any apparent business purpose.
  - Frequent cash deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
  - Large cash deposit is followed within a short time by wire transfers to high-risk jurisdictions.
  - Numerous cash deposits made in different bank branches over a short period of time.
  - Frequent cash deposits in small amounts, without any apparent business purpose or reasonable grounds.
  - Customers who use false identification or offer different identifications on separate occasions

2.3.1.3 Currency Exchanges

Cash-intensive businesses may include currency exchanges as legitimate providers of services. Currency exchanges, however, can also be an attractive vehicle that illicit actors seek to exploit to enter the financial system and transfer their funds. According to the FATF, the simplicity and certainty of currency exchanges transactions and the anonymity and portability of cash make them attractive to money laundering and the financing of terrorism and illegal organisations.[5] Once the money has been exchanged, it is difficult to trace its origin. There are two different ways to perform a currency exchange: (1) the use of cash to exchange and transfer the funds; or (2) the use of the internet to perform the currency exchange and transfer the funds to a bank account.

- **Potential Risk Indicators:**
  - Significant and/or frequent local or foreign currency exchanges.
  - Opening of foreign currency accounts with no apparent business or economic purpose.
  - Customers who know little about or are reluctant to disclose details about the payee, or customers or parties with no apparent ties to the destination country.
  - Suspicion that the customer is acting on behalf of a third party but not disclosing it.
  - Transactions involving charities and other non-profit organizations, which are not properly licensed or registered. It is reminded that when opening any accounts for non-profit organisations, LFIs must obtain an original signed letter from the Ministry of Community Development for opening accounts to collect donations and an authorization from the UAE

[5] FATF "Money Laundering through Money Remittance and Currency Exchange Providers" (June 2010), available at: https://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf

Red Crescent for conducting financial transfers out of the UAE through some of these accounts.
- Customers who use false identification or offer different identifications on separate occasions.
- Customers who receive transfers in seasonal patterns or transactions in a pattern consistent with criminal proceeds.

3. Mitigating Risks

Effective risk mitigation is critical to protecting the LFI, complying with its legal obligations, and meeting supervisory expectations. When establishing and maintaining relationships with cash-intensive businesses, LFIs should establish policies, procedures, and processes to identify higher-risk relationships, assess AML/CFT risks of the cash-intensive business, conduct due diligence at account opening and throughout the relationship, and monitor these relationships for unusual or potentially suspicious activity. When performing a risk assessment of cash-intensive businesses, LFIs should allocate resources to those accounts that pose the greatest risk of money laundering or financing of terrorism and illegal organisations. To that end, LFIs should understand their risk and take effective, risk-based steps to protect themselves from abuse and from illicit actors and transactions.

The sections below discuss how LFIs can apply specific preventive measures to identify, manage, and mitigate the risks associated with cash-intensive businesses. LFIs should consult the legal and regulatory framework currently in force, the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions*, and the CBUAE issued Guidances for further information.[6] The controls discussed below should be integrated into the LFI's larger AML/CFT compliance program and supported with appropriate governance and training.

3.1 Risk-Based Approach

LFIs must take a risk-based approach to the preventive measures they put in place for all customers, including cash-intensive businesses. A risk-based approach means that LFIs should dedicate compliance resources and effort to customers, business lines, branches, and products and services in keeping with the risk presented by those customers, business lines, branches, and products and services, as assessed in accordance with Article 4 of AML-CFT Decision. **The risk-based approach has three principal components**:

3.1.1 Conducting an Enterprise Risk Assessment

As required by Article 4.1 of AML-CFT Decision, the enterprise risk assessment must reflect the presence of higher-risk customers, including cash-intensive business customers, in an LFI's customer base. These assessments should in turn be reflected in the LFI's inherent risk rating. In addition, the LFI's controls risk assessment should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed by its cash-intensive business customers, including the preventive measures discussed below.

[6] Available at https://www.centralbank.ae/en/cbuae-amlcft.

3.1.2 Identifying and Assessing the Risks Associated with Specific Customers

The LFI is expected to assess the risk of each customer to identify those that require EDD and to support its entity risk assessment. In assessing the risks of a cash-intensive business, LFIs should consider:

i. **Geographic Risk:** LFIs should assess the risks associated with the jurisdictions in which the business is registered/headquartered and where it operates, including the jurisdictions where it has subsidiaries, where it sources its products (where relevant), and where its main counterparties are based. These may include the overall risk of money laundering, financing of terrorism and illegal organisations, and financing of proliferation, as well as what is known regarding the prevalence of abuse of entities in these sectors. There are a number of sources that LFIs can use to develop a list of high-risk countries, jurisdictions, or regions. LFIs should consult any publications issued by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee (NAMLCFTC)[7], the UAE Financial Intelligence Unit (UAE FIU), and the FATF, including the FATF's list of jurisdictions subject to countermeasures and to increased monitoring. LFIs may also use public free databases such as, for example, the Basel AML Index[8] or the Transparency International Corruption Perceptions Index.[9] LFIs should not solely rely on public lists, however, and should consider their own experiences and the nature of their exposure to each jurisdiction when assessing the risk of that jurisdiction.

ii. **Customer Risks:** LFIs should assess the type of cash-intensive business, the maturity of that relationship (if the relationship is a long-term business relationship of the LFI), and other characteristics of the business relationship, such as the customer's ownership structure. Cash-intensive businesses that have a complex legal ownership structure, for example, may be higher risk than those with simpler ownership structures.

iii. **Product, Service, and Delivery Channel Risk:** LFIs should assess risk in this category based on the products and services that the customer intends to use, and the delivery channels through which the LFI will provide these services. LFIs should draw on their entity risk assessment to assess the risk of the products and services each customer uses or intends to use. (See also Section 3.2.3 below in relation to understanding the nature of the customer's business and purpose of the business relationship.)

Questions that an LFI may ask to determine the risk profile of a cash-intensive business include, but are not limited to:

- Where is the business incorporated? Where does it operate? Are these high-risk jurisdictions?
- What type of industry does the cash-intensive business operate in?
- What types of products and services is the business requesting?
- What is the intended volume, frequency, and nature of cash transactions that the cash-intensive business intends to conduct through its account?
- What is the regulatory environment in the jurisdiction(s) where the cash-intensive business is incorporated/has operations?

[7] Available at: https://www.namlcftc.gov.ae/en/high-risk-countries.php
[8] Available at: https://baselgovernance.org/basel-aml-index
[9] Available at: https://www.transparency.org/en/cpi/2020/index/nzl

- What is the ownership structure of the customer? Do the customer's beneficial owners, shareholders, directors, and senior managers reside in a high-risk jurisdiction?
- What is the availability of information on the customer? Is the customer cooperating with the LFI to provide all the necessary customer due diligence ("CDD")/EDD information to the LFI?
- If the customer is an existing customer, does the customer have a history of Suspicious Transaction Report ("STR") filings?

3.1.3 Applying EDD and other Preventive Measures

Where the LFI determines a customer to be higher-risk, Article 4.2(b) of AML-CFT Decision requires that the LFI apply EDD. EDD is also required for specified higher-risk customer types, no matter their risk rating:

- Customers who are Politically Exposed Persons ("PEPs") or that are owned or controlled by PEPs;
- Customers from higher-risk jurisdictions; and
- Customers with whom the LFI is establishing a correspondent relationship.

EDD measures should be designed to mitigate the specific risks identified with particular customers. Examples of EDD measures are described below in Section 3.2.

3.2 Customer Due Diligence and Enhanced Due Diligence

CDD, and where necessary EDD, are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers. As discussed below, each stage of the CDD process gives LFIs an opportunity to collect the information they need to identify and manage the specific risks of higher-risk customers.

The goal of the CDD process is to ensure that LFIs understand who their customer is and the purpose for which the customer will use the LFI's services. **Where an LFI cannot satisfy itself that it understands a customer, then it should not accept it as a customer. If there is an existing business relationship, the LFI should not continue it. LFIs should also consider filing a STR**, as discussed in Section 3.3.2.

Under Article 5 of AML-CFT Decision, LFIs should conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship. Although Article 5 permits CDD to be delayed in circumstances of lower risk, the potential higher risk of cash-intensive businesses makes it unlikely that delayed CDD will be appropriate in the context of onboarding such customers. To this end, at the time of account opening, the LFI should seek to understand the cash-intensive business' operations and business structure, the intended use of the account (including anticipated transaction volume, products, and services used), the geographic location(s) involved in the relationship, and jurisdiction(s) of operations. As part of collecting this information, the LFI should also assess the availability of information on the cash-intensive business and cooperation of the business in providing information to the LFI.

The following elements of CDD should be carried out for all customers, no matter the customer type.

3.2.1 Customer Identification and Verification

Under Article 8 of AML-CFT Decision, LFIs are required to identify and verify the identity of all customers. As stipulated in the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions*, the identification and verification of the identity of customers is a fundamental component of an effective ML/FT risk management and mitigation program. Please see Section 6.3.1 of the above-mentioned Guidelines for further information on customer identification.

3.2.2 Beneficial Owner Identification

The majority of cash-intensive businesses will be legal persons. Article 9 of AML-CFT Decision requires all financial institutions to identify the beneficial owners of a legal person customer by obtaining and verifying the identity of all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. Where no such individual meets this description, the LFI should identify and verify the identity of the individual(s) holding the senior management position in the entity.

The beneficial owner of a legal person must be an individual. Another legal person cannot be classified as the beneficial owner of a customer, no matter what percentage it owns. LFIs should continue tracing ownership all the way up the ownership chain until it discovers all individuals who own or control at least 25% of the LFI's customer. When the LFI has identified qualifying beneficial owners, it should perform CDD on each individual beneficial owner, in accordance with the requirements of Article 8.1(a) of AML-CFT Decision (10). If no individual qualifies as a beneficial owner, LFIs should identify the individual(s) holding the position of senior management officer(s) within the customer. This option should be used only as a last resort, however, and when the LFI is confident that no one individual, or small group of individuals, exercises control over the customer. Please see the CBUAE's *Guidance for LFIs providing services to Legal Persons and Arrangements*[10] for more information on identification of beneficial owners.

3.2.2.1 EDD: Beneficial Ownership

If the LFI has followed the steps described above and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so is to identify additional beneficial owners below the 25% ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10% or even the 5% level, as risk warrants. It should also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

3.2.3 Nature of the Customer's Business and Purpose of the Business Relationship

Under article 8 of AML-CFT Decision, for all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This step requires the LFI to collect information that allows it to create a profile of the customer and of the

[10] Available at https://www.centralbank.ae/en/cbuae-amlcft.

expected uses to which the customer will put the LFI's products and services. This element of CDD will have important implications for the customer risk rating.

It is critical that LFIs have processes and controls in place to ensure that they are able to identify cash-intensive business customers. In line with a risk-based approach, LFIs should interview the customer, review the customer's business license, request recent financial statements (audited if available), tax returns or additional information, search company databases and assess the primary business activity, products, and services offered by the customer to understand the full scope of the customer's business.

If an LFI determines that a customer or prospective customer has materially misrepresented itself or its business, it should not onboard the customer and should exit the relationship if one has been established. In addition, the LFI should consider filing a Suspicious Transaction Report (STR), Suspicious Activity Report (SAR) or other report types to the UAE FIU as discussed in section 3.3.2 below. The LFI may also consider adding the customer, its beneficial owners, directors, and its managers to internal watchlists.

High-risk customers should be treated as high risk no matter the financial services they use. Even so, the risk to which the LFI may be exposed can vary based on the purpose of the account and the types of financial products and services the customer wishes to use. LFIs should fully understand the uses to which the cash-intensive business intends to put the account and the expected activity on the account, to the extent that it can generally predict activity on the account and identify activity that does not fit the profile. To that end, the LFI should seek to assess the expected volume, frequency, and nature of cash transactions that the customer intends to conduct through its account, as this will be an important risk factor for identifying money laundering and financing of terrorism and illegal organisations risks associated with the cash-intensive business. In addition, the LFI may wish to consider whether the expected volume of cash coming through the account is consistent with the declared sales income and whether the expected volume of cash appears reasonable compared to other similar cash-intensive customers of the LFI (i.e., operating as similar business types in similar markets).

3.2.4 Ongoing Monitoring

Under Article 7 of AML-CFT Decision, all customers must be subject to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

3.2.4.1 CDD Updating

LFIs are expected to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. This is particularly crucial in the context of customers that are companies or that engage in cash-intensive business. The risk associated with a cash-intensive business can change overnight if the customer changes its business activities. LFIs should update CDD for all customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

CDD updates should include a refresh of all elements of initial CDD, and in particular should ascertain that:

- The customer's beneficial owners remain the same;

- The customer continues to have an active status with a company registrar;
- The customer has the same legal form and is domiciled in the same jurisdiction; and
- The customer is engaged in the same type of business, and in the same geographies.

In addition to a review of the customer's CDD file, the LFI should also review the customer's transactions to determine whether they continue to fit the customer's profile and business and are consistent with the business the customer expected to engage in when the business relationship was established. In this capacity, the LFI should pay particular attention whether the volume of cash coming through the account is consistent with the declared sales income of the cash-intensive business customer. This type of transaction review is distinct from the ongoing transaction monitoring discussed below. The purpose of the review is to complement ongoing transaction monitoring by identifying behaviours, trends, or patterns that are not necessarily subject to transaction monitoring rules.

The techniques used for transaction review will vary depending on the customer. For lower-risk customers, a review of alerts, if any, is likely to be sufficient. For higher risk customers, such as cash-intensive businesses rated as high-risk, a more intensive review may be necessary. For customers with a large volume of transactions, LFIs may use data analysis techniques to identify unusual behaviour. If the review finds that the customer's behaviour or information has materially changed, the LFI should risk-rate the customer again. New information gained during this process may cause the LFI to believe that EDD is necessary or may bring the customer into the category of customers for which EDD is mandatory (i.e., customers that are PEPs; customers that are based in high-risk jurisdictions; etc.).

LFIs may consider requiring that the customer update them as to any changes in its beneficial ownership or business activities. Even if this requirement is in place, however, LFIs should not rely on the customer to notify it of a change but should still update CDD on a schedule appropriate to the customer's risk rating.

3.2.4.2 EDD: Ongoing Monitoring

When customers are higher risk, such as for cash-intensive businesses rated as high-risk following the completion of the CDD process, monitoring should be more frequent, intensive, and intrusive. LFIs should review the CDD files of higher risk customers on a frequent basis, such as every six or nine months for very high-risk customers. The methods LFIs use to review the account should also be more intense and should not rely solely on information supplied for the customer. For example, LFIs should consider:

- Reviewing more or all transactions on the account, rather than a sample of transactions;
- Conducting site visits at the customer's premises, whenever the LFI is not satisfied with the documentation provided by the customer, and requesting a meeting between an appropriate LFI representative and the customer's managing director or Chief Financial Officer. Site visits can be particularly important for certain cash-intensive businesses, including those that use an LFI's cash management services on a large scale, as they allow the LFI's compliance personnel to inspect the institution's cash management program and the controls it has in place to prevent illicit cash being commingled with legitimate funds; and
- Conducting searches of public databases, including news and government databases, to independently identify material changes in a customer's ownership or business activities or to identify adverse media reports. Such searches should include adverse media searches of public

records and databases, using relevant key words, including but not limited to, allegation, fraud, corruption, laundering.

3.3 Transaction Monitoring and STR Reporting

3.3.1 Transaction Monitoring

Under Article 16 of AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of a suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types. As with all customer types, LFIs that use automated monitoring systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behaviour. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD, including the identities of beneficial owners. For example, a series of transactions between two unconnected companies may not be cause for an alert. But if the companies are all owned or controlled by the same individual(s), the LFI should investigate to make sure that the transactions have a legitimate economic purpose. In addition, higher-risk customers should be subject to more stringent transaction monitoring, with lower thresholds for alerts and more intensive investigation.

Monitoring systems can include manual monitoring processes and the use of automated and intelligence-led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/TF risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated to the size, nature, and complexity of each institution. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening* for further information.[11]

The transaction monitoring system used by LFIs should be equipped to identify patterns of activity that appear unusual and potentially suspicious for cash-intensive business customers as well as unusual behaviour that may indicate that a customer's business has changed in such a way as to require a high-risk rating. Some red flags for cash-intensive business customers are described below. If an LFI's automated transaction monitoring system is not capable of alerting on these red flags, LFIs should have in place manual monitoring, such as management information systems.

- The business engages in significantly greater volumes of cash transactions in comparison to other similar business types operating in similar jurisdictions and markets.
- The business engages in unusually frequent domestic and international ATM activity.
- The customer makes a cash deposit followed by an immediate request that the money be wired out or transferred to a third party, without any apparent business purpose.
- There are frequent cash deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
- The parties to the transaction (e.g. originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
- The customer uses a personal/individual account for business purposes or vice versa.

[11] Available at https://www.centralbank.ae/en/cbuae-amlcft.

- Upon request, a customer is unable or unwilling to produce appropriate documentation (e.g. invoices) to support a transaction, or documentation appears doctored or fake (e.g. documents contain significant discrepancies between the descriptions on the invoice, or other documents such as the certificate of origin or packing list).
- The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to high-risk jurisdictions.
- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

3.3.2 STR Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file a suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types with the UAE Financial Intelligence Unit ("UAE FIU") when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. **STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system.** STR filings assist law enforcement in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a crime, LFIs should consider filing an STR in the following situations involving higher-risk customers:

- A potential customer decides against opening an account or purchasing other financial services after learning about the LFI's CDD requirements;
- A current customer cannot provide required information about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty; or
- The LFI is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the LFI should not establish the business relationship, or continue an existing business relationship.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*[12] for further information.

3.4 Governance and Training

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective. Additionally, the LFI's senior management must clearly endorse and support the AML/CFT program.

[12] Available at https://www.centralbank.ae/en/cbuae-amlcft.

As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of cash-intensive business customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. For example, an LFI that has a large number of cash-intensive business customers should offer training that includes an in-depth discussion of risk factors and red flags related to such customers.

Annex 1. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this guidance is to assist Licensed Financial Institutions (LFIs) understand and mitigate the risks when providing services to customers who are cash-intensive businesses (CIBs), and to guide them in fulfilling their AML/CFT obligations. The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that, as the UAE is a cash-intensive economy and plays an important part in global trade, there are significant risks associated with the cross-border movement of cash and bearer negotiable instruments.
	Applicability	This guidance applies to natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories: • all national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and • insurance companies, agencies, and brokers.
Understanding Risks	Vulnerabilities of Cash	The specific characteristics of cash—its anonymity, interchangeability, and transportability—make it an attractive option for illicit actors seeking to conceal the proceeds of crime. Cash holds no record of its source or owner and can be easily concealed in large quantities. Cash transactions are also instantaneous and widely accepted across jurisdictions.
	Vulnerabilities of Alternatives to Cash	Illicit actors also use various monetary instruments in conjunction with, or as a replacement to, cash. Both bearer negotiable instruments and prepaid cards, for instance, offer similar benefits to cash, including anonymity and accessibility. They can store large amounts of value in a compact physical size that is easily transportable and obscures the origin of the funds. • Bearer negotiable instruments are financial instruments of whatever form, whether in the form of a bearer document, such as traveler's cheques, promissory notes and cheques, payment orders, or others. • Prepaid cards can be used as an alternative to cash in that they provide access to funds that have been paid in advance. Funds can be claimed or transferred through an electronic device, such as through a card, code, electronic serial number, mobile identification number, or personal identification number within either an *open* or *closed* loop system.
	Vulnerabilities of Cash-intensive Businesses	**Types of CIBs:** CIBs are businesses that experience a high volume of cash flows. CIBs span across various industry sectors and most are operating a legitimate business. However, some aspects of these businesses may be vulnerable to money laundering or the financing of terrorism and illegal organisations. Examples of cash-intensive businesses that can pose a higher risk include but are not limited to: convenience and retail stores; restaurants; wholesale and general trading businesses; travel agencies and tour operators and car dealers. LFIs may expand on the above by considering additional factors when identifying cash-intensive businesses in their customer base and should consider the specific risks posed by the below features to determine whether the customer is considered as high-risk and should be subject to enhanced due diligence ("EDD") measures.
		Cross-Border Movement of Cash and Cash Couriers: CIBs may move cash across borders as part of their business model including by utilizing cash couriers. Cross-border movement of licit cash can be legal, subject to compliance with reporting and other relevant legal and regulatory requirements. However, criminals may also seek to move cash across borders to launder proceeds of crime by placing them in another jurisdiction. Natural of legal persons must declare upon entering or leaving the UAE any currencies, bearer negotiable instruments, precious metals and stones above the threshold of AED 60,000. Understanding whether customers have made any such declarations, in accordance with the Regulation should form part of any due diligence by the LFIs where required.
		Cash Deposits: CIBs can be expected to make cash deposits, which is legal and a natural fit with their business model. Illicit actors, however, will also seek ways to place their illicit cash into the financial system. Terrorists also seek to finance, often through small amounts of cash, activities without traceability. LFIs should, as the case may be, undertake CDD measures on the third party cash depositors transacting in any accounts above the threshold specified in Article 6 of the AML-CFT Decision. LFIs should also obtain appropriate information regarding the source of cash deposited in a customer's account as well as mandate the use of Emirates ID for cash deposits in ATMs.
		Currency Exchanges: CIBs may include currency exchanges as legitimate providers of services. Currency exchanges, however, can also be an attractive vehicle for illicit actors seeking to enter the financial system and transfer their funds. Once the money has been exchanged, it is difficult to trace its origin.

Mitigating Risks	Risk-Based Approach	LFIs must take a risk-based approach in their AML programs. This means that they should assess all customers, including CIB customers, to determine their degree of risk. The LFI is expected to assess the risk of each customer to identify those that require EDD and to support its entity risk assessment. In assessing the risks of a cash-intensive business, LFIs should consider: • Geographic Risk related to the jurisdiction(s) in which the customer is based and where it operates; • Customer Risks related to the customer's customer base, incl. its type and the characteristics of the business relationship; and • Product, Service, and Delivery Channel Risk related to the products and services the customer intends to use and the delivery channels through which the LFI will provide these services.
	Customer Due Diligence and Enhanced Due Diligence	For all customers, including CIB customers, LFIs must perform Customer Due Diligence ("CDD") with the following components:
		Customer Identification: LFIs are required to identify and verify the identity of all customers. Please see the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions* for further information on customer identification.
		Beneficial Owners identification: The majority of cash-intensive businesses will be legal persons. For all legal person customers, LFIs must identify all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. If no such individual can be identified, the LFI must identify the individual(s) holding the senior management position(s) within the legal person customer.
		Nature of the Customer's Business and Purpose of the Business relationship: The purpose of the account and the nature of the customer's business are critical drivers of risk for CIB customers. LFIs should fully understand the uses to which the CIB intends to put the account and the expected activity on the account, to the extent that it can generally predict activity on the account and identify activity that does not fit the profile. As they seek to understand the customer's business, LFIs should collect all information necessary to assess customer risk.
		Perform Ongoing Monitoring: For all customers, LFIs should ensure that the customer information is accurate, complete and up-to-date, and that the customer's profile and business are consistent with the expectations set at onboarding. If not, the customer risk rating may need to be changed. When customers are higher risk, such as for cash-intensive businesses rated as high-risk following the completion of the CDD process, monitoring should be more frequent, intensive, and intrusive.
	Transaction Monitoring and Suspicious Transaction Reporting	The transaction monitoring system used by LFIs should be equipped to identify patterns of activity that appear unusual and potentially suspicious for CIB customers as well as unusual behaviour that may indicate that a customer's business has changed in such a way as to require a high-risk rating. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening* for further information. LFIs must file a suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types with the UAE Financial Intelligence Unit ("UAE FIU") when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.
	Governance and Training	The preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of cash-intensive business customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls.