CBUAE Classification: Public

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 ON THE RISKS RELATING TO PAYMENTS

August 1, 2022

Contents

1. Introduction

1.1. Purpose of the Guidance

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 Illicit Organizations 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[2] 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; and
- Stored value facilities, retail payment service providers, and card schemes.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.
[2] FATF: *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services, 2013,* https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf, and *Correspondent Banking Services, 2016*, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws:

- Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended by Decree Federal Law No. (26) of 2021 ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended by Cabinet Decision No. (24) of 2022 ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74").

1.4. Acronyms and Definitions

Card Scheme: a single set of rules, practices and standards that enable a holder of a payment instrument to effect the execution of card-based payment transactions within the UAE which is separated from any infrastructure of payment system that supports its operation, and includes the card scheme governing body. For the avoidance of doubt, a card scheme may be operated by a private or public sector entity.

Correspondent Banking Relationship: the relationship between a correspondent financial institution and a respondent one through a current account or any other type of account(s) or through a service related to such an account and includes a corresponding relationship established for the purpose of securities transactions or transfer of funds.

Nesting: defined by the FATF as the use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

New Payment Products and Services (NPPS): defined by the FATF as new and innovative payment products and services that offer an alternative to traditional financial services.

Payment Sector: refers to different forms of payment that are transmitted and exchanged across various delivery channels, frequently utilizing digital platforms, systems, services and products.

PPS: Payment Products and Services.

Retail Payment Services: any of the following services: payment account issuance; payment instrument issuance; merchant acquiring; payment aggregation; domestic fund transfer; cross-border fund transfer; payment token; payment initiation; and payment account information.

Stored Value Facility (SVF): a facility (other than cash) for or in relation to which a customer, or another person on the customer's behalf, pays a sum of money (including money's worth such as values, reward points, crypto-assets or virtual assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including money's worth such as values, reward points, crypto-assets or virtual assets) whether in whole or in part, on the facility; and (b) the relevant undertaking. SVF includes device based SVF and non-device based SVF.

2. Understanding Risks

There is no uniform global approach to regulation of the Payment Sector and participants may be classified as different types of entities in different regulatory regimes. Some types of participants may be regulated as financial institutions in some jurisdictions but not in others. Operating within a global financial center, LFIs in the UAE may be exposed not just to participants licensed by the CBUAE, but also to those operating globally. This exposure can be direct (i.e., providing financial services directly to a participant), or indirect (e.g., when a customer initiates a withdrawal from his checking account using a foreign smartphone-based app that he has linked to that account).

The Payment Sector is becoming increasingly diverse, and payment processes more complex. The Payment Sector is no longer solely dominated by traditional financial institutions like banks and exchange houses, which also offer new and innovative methods using the internet or mobile phone technology. A variety of new types of Payment Sector participants, such as companies that offer internet-or smartphone-based payment applications and providers of prepaid cards and devices, are involved in a growing percentage of all payment transactions. These entities allow almost anyone to accept and originate payments using a wide variety of techniques and payment routes. Whenever a customer makes a purchase or pays a bill online, these new participants are likely to be involved. These entities may also be used outside commercial contexts, such as by crowdfunding platforms or charitable organizations.

Furthermore, as innovative technologies emerge and commerce and economic activity increasingly grows online, merchants and consumers are relying on a diverse array of New Payment Products and Services (NPPS). The FATF defines NPPS as "*new and innovative payment products and services that offer an alternative to traditional financial services*." Examples of NPPS include prepaid cards, mobile payments, and internet-based payment services; these are neither exhaustive, nor exclusive as a provider of mobile money, for instance, may utilize prepaid cards or provide internet-based payment services. In contrast, payment methods such as credit cards and cheques, and bulk funds transfer systems such as national payment systems, would generally not qualify as NPPS. Because NPPS are so diverse, they do not share a single risk profile and pose money laundering and financing of terrorism (ML/FT) risks for financial institutions when they do not understand the operation or the vulnerabilities in the NPSS operational models. The provision of these NPPS is frequently implemented or facilitated by a group or network of different companies, some of them invisible to the consumer or even all the participants in the network, given the presence of multiple participants in the chain with whom not all participants will have a contractual relationship.

The vast majority of payment transactions carried out each year across the globe are legitimate. But the Payment Sector—and NPPS in particular—has characteristics that make it both attractive and vulnerable to illicit actors. As LFIs are increasingly exposed to new participants in this sector, they must remain alert to and understand the risks this exposure creates.

Section 2.1 below discusses the ML/FT risks of the Payment Sector with a focus on risks related to NPPS. It applies to financial institutions that are directly involved in the provision of such products and services, which includes both traditional LFIs and those that are solely engaged in providing payments. Section 2.2 discusses risks specific to LFIs that provide services to other Payment Sector participants.

2.1. ML/FT Risks of the Payment Sector

2.1.1. Characteristics of the Movement of funds

PPS, and NPPS in particular, are extremely attractive to illicit actors because of the rapid movement of funds between Payment Sector participants and across borders. The risks of a specific payment network or application however can vary based on the features that make it more or less attractive to illicit actors, such as:

- **Transaction speed.** Are transactions instantaneous, or do they take hours or days? The quicker the transaction, the easier it is for illicit actors to conduct multiple transfers, further obscuring the origin of the funds, before coming to the attention of the authorities.
- **Transaction limits**. Does the PPS have transaction caps or limits? Smaller-value payments are not without risk, especially in the terrorist financing context, but they do make it more difficult to move illicit funds on a large scale.
- **Closed vs open loop system**. PPS, primarily SVF, can be "closed" or "open" loop. In a closed loop system, the payment method can only be used for payments to a specific payee. Examples include transit passes and store gift cards. In an open loop system, the payment method can be used to pay a wide variety of payees, and can be linked to other payment methods that further expand its reach. Although it is certainly possible to use closed loop systems for ML/FT (for instance, if a terrorist group collects store gift cards and uses them to purchase equipment), the restrictions on their use makes them less attractive to illicit actors.
- **Methods of funding and access to cash**.[3] The methods by which a PPS can be funded (such as by cash, through another payment service, a prepaid model, or by third-party funding from anonymous sources) may increase risk. The inputs and outputs of a given PPS are therefore an important consideration when assessing risk, including whether the funding source is located internationally such as a high-risk country. For example, illicit actors may seek to place cash in the financial system or to obscure transaction trails by converting funds in and out of cash. PPS that permit users to fund their accounts with cash, or that allow users to withdraw cash, may be higher risk. In addition, as discussed above in the context of open loop systems, the more open and porous the PPS, the higher the risk it may present. PPS that allow users to fund accounts from multiple sources, and to withdraw funds using multiple methods, are likely to be more attractive to illicit actors, and will be harder to effectively monitor.
- **Payment transparency**. NPPS often have aggregated payments and settlement accounts involving multiple parties and long payment chains thereby potentially causing LFIs to have reduced visibility into payment activity taking place through the PPS as well as obscuring an LFI's ability to identify the ultimate payer and payee for all transactions.
- **Ability for one person to create multiple accounts.** Some PPS allow customers to create multiple accounts using the same ID. These may be individual accounts or created on behalf of minors or other family members. Illicit actors may seek to rapidly cycle funds through accounts (whether or not these take the form of virtual 'wallets' or other SVF) in order to obscure payment trails. They may also seek to open multiple accounts to facilitate fraud and other criminal activity.

[3] For details on the vulnerabilities of cash and alternatives to cash, please consult the CBUAE's *Guidance for Licensed Financial Institutions providing services to Cash-Intensive Businesses*

Restricting a customer to one account does not eliminate risk, since illicit actors often work in groups, but it makes it more difficult for a single person to launder funds by conducting a self-transfer.

- **Non-face-to-face relationships**. Does the payment method allow for a non-face-to-face business relationship? What are the payment method's characteristics? Can the relationship be established through agents, online or through a mobile payment system? The absence of contact and/or anonymity may increase the risk of identity fraud or customers providing inaccurate information.
- **Use of virtual assets**.[4] As interest in virtual assets grows, more and more payment methods and schemes are integrating with virtual assets. For example, a global payments firm allow users in some countries to purchase virtual assets using the funds in their account, although not to use them directly for payments. Payment methods and schemes that integrate virtual assets could expose financial institutions to the specific risks of this sector.

2.1.2. Peer-to-Peer Payments

NPPS have revolutionized the ability to make payments or transfer funds. Where cash transactions previously required face-to-face interaction and bank transfers involved transactions' fees and an execution time in the past, NPPS allow participants to send money that will be instantly available to the beneficiary, reducing the need for trust in the relationship. As a result, the availability of convenient, inexpensive PPS has led to a decreasing use of cash, particularly in highly developed countries. **Bringing transactions into the formal financial system has many advantages from the perspective of combating illicit finance.** These transactions can flow through third parties that are in many cases subject to AML/CFT requirements. In most cases, the payments that involve such third parties include information on the payer and the payee and are permanently recorded by a financial institution, making it easier for law enforcement to track transactions. But the use of PPS for peer-to-peer payments also creates risk for financial institutions because it means that many smaller illicit transactions that once took place in cash are now being conducted via PPS, particularly NPPS.

2.1.3. Cross-Border Movement

One of the principal features of many NPPS is that they can be used globally for making payments or transferring funds. While the usefulness of cash and cheques is limited outside the jurisdiction where they were issued, many PPS are internet-based services and specialize in conducting transfers between countries and currencies. For example, a UAE bank that offers checking accounts to UAE residents may have no ATMs or branches outside the UAE. But, if users link their accounts to global or regional payment apps, they can conduct transactions with persons over the world and can use their smartphone as a payment instrument in countries where the bank has no presence, thus introducing new geographical exposure potentially to high-risk countries. And **unlike cross-border wires, which carry full identifying information,** the bank will frequently only see the customer's transactions with the payment network itself, rather than their location or ultimate destination. Many illicit finance schemes involve the cross-border movement of funds. Criminals may seek to finance terrorism in other countries, move funds out of sanctioned jurisdictions, or evade the attention of law enforcement in the jurisdiction where a proceeds-

[4] Please note that the risks relating to Virtual Assets/Virtual Assets Service Providers are out of the scope of this guidance and addressed in a separate guidance to be issued by the CBUAE.

generating offense was committed. PPS that allow or facilitate cross-border movement of funds may therefore be particularly attractive to illicit actors.

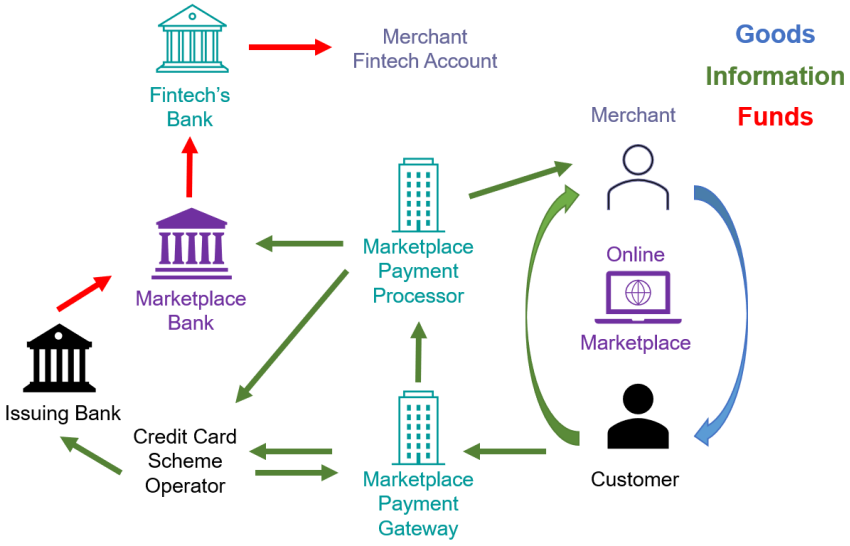
2.1.4. Global Regulatory Gaps

Countries take a variety of approaches to regulating the Payment Sector and there is no one widely accepted classification of participants. As a result, two regulators in two different jurisdictions may subject a single company to very different requirements based on each jurisdiction's regulatory framework. The company may be regulated as a financial institution in one jurisdiction, and thus subject to AML/CFT requirements, but treated as a tech company in another with no requirement to apply preventive measures. Companies may provide services to customers in a given country without being regulated in that country at all. Even where Payment Sector participants are fully regulated and subject to stringent AML/CFT requirements, supervisors' expectations for this sector may be lower than for traditional financial institutions such as banks. And participants, as relatively new market entrants, may lack the experience, expertise, or commitment to apply fully effective preventive measures. These entities may be less able to protect themselves and their partners, and thus vulnerable to abuse by illicit actors.

2.1.5. Intermediation

The Payment Sector may be complex with a number of participants potentially involved in a single transaction. As a result, many payment transactions will be highly intermediated, with multiple financial institutions involved in a funds transfer. Additional entities (some of which may not be financial institutions) can potentially facilitate the transaction through the exchange of information. Intermediated transactions create risk because no regulated entity participating in the transaction has the visibility necessary to fully understand the transaction and the participants. Illicit transactions may have red flags when viewed as a whole, but may appear legitimate when seen from the perspective of each of the financial institutions involved. This creates a vulnerability that illicit actors can exploit.

For example, consider the hypothetical transaction below, a purchase on an online marketplace that allows individual sellers to sell items directly to customers:



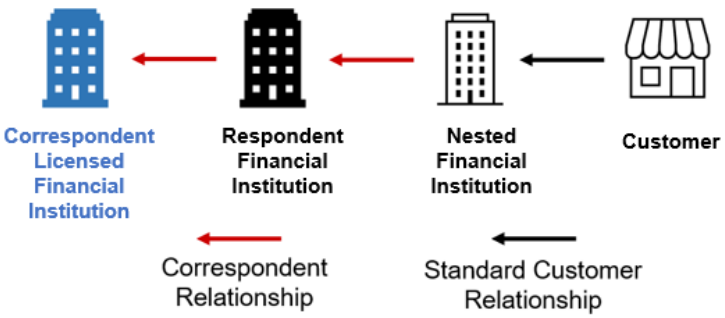
In this transaction, the customer is using a credit card to purchase goods from the merchant, but the merchant is not a participant in the credit card scheme. A number of Payment Sector participants help to bridge this gap and facilitate the transaction:

- The marketplace uses a payment gateway that accepts the customer's credit card credentials, encrypts them, and validates them against data held by the credit card scheme operator. The marketplace may also integrate with providers that provide 'one-click' payment information to the payment gateway without requiring the customer to enter his or her credit card details. In the UAE, these providers would be classified as conducting payment account information services, but in many other jurisdictions they are not regulated as financial institutions.
- The credit card scheme operator validates the customer information provided by the payment gateway, conducts initial fraud checks, and informs the payment gateway that the credit account is in good standing and the credit limit has not been exceeded.
- The payment gateway informs the marketplace's payment processor that a transaction of an identified value can proceed using the customer's credit card details.
- The marketplace payment processor informs the merchant that the transaction has been confirmed and instructs the credit card scheme operator to debit the customer's account for the purchase price, in favor of the marketplace.
- The credit card scheme operator passes this payment instruction on to the bank that issued the customer's credit card (the issuing bank). Meanwhile, the merchant ships the customer the merchandise purchased.
- The issuing bank transfers funds in the purchase value to the marketplace's bank (this transfer may in fact go through the marketplace payment processor's account at the same bank).
- The marketplace bank transfers the purchase funds to the merchant's fintech (likely a provider of SVF), which in turn transfers the funds to the merchant's account. The marketplace's payment processor likely facilitates this transaction by instructing the bank where to send the funds.

It is unlikely that any of the Payment Sector participants in this transaction have full visibility into the funds transfer chain. The banks are unlikely to have information on anyone other than their immediate customers or correspondents. The payment gateway likely does not identify the merchant. The fintech likely does not identify the customer. The marketplace payment processor is likely aware that the customer and merchant are engaging in a transaction, but may not know where the customer's funds are coming from or where the merchant's funds are going. And because the marketplace payment processor does not hold funds at any point in the transaction, it may not be regulated as a financial institution in all jurisdictions. In this instance, a marketplace payment processor may apply certain conditions on what types of customers and merchants it engages. For more information on how LFIs can mitigate and manage ML/FT risks related to this sector, including the risks arising from the use of NPPS, please see section 3 "Mitigating Risks."

2.1.6. Nesting

Nesting is a form of intermediation that presents specific risks. In most Correspondent Banking Relationships that involve nesting, the respondent financial institution is not aware of individual transactions ordered by the ultimate customer; instead, the respondent sees bulk activity in the correspondent's account that represents aggregate customer orders and perhaps also proprietary transactions by the correspondent. As a result, the transaction is intermediated because the respondent cannot see—nor assess the risk of—the original customer.



Although nesting can occur in the context of any financial service, some features of the Payment Sector—the long payment chains and the involvement of multiple parties—can increase the likelihood that nesting will take place. In particular, some Payment Sector participants specialize in providing financial services to dubious merchants or customers who would be rejected by larger financial institutions. A participant servicing these customers, frequently offering merchant acquiring or payment aggregation services, will establish a nested relationship with a third participant that in turn has a Correspondent Banking Relationship with a bank. Although all the parties involved must and may claim to perform appropriate merchant due diligence, in practice, the risk may be that the bank is relying on its correspondent, which is in turn relying on the nested financial institution, with the first two parties not having full visibility into the nested financial institution's customer base or due diligence practices.

2.1.7. Use of Agents and Affiliates

Payment Sector participants often interact in a dense web of agency and affiliate relationships, with each participant playing a defined role. A large number of entities involved in the NPPS, in particular when involving several countries, may increase the ML/FT risk.

For example, entities involved in the provision of SVF through a prepaid card scheme could include:[5]

- The issuer of the SVF, such as the issuer of prepaid cards, who is accountable to the customer for holding the funds they have loaded into the SVF (issuers are often banks that maintain program funds in a single program account);
- The merchant acquirer (or acquirers), who establishes a direct relationship with merchants, distributes and maintains the payment gateway, collect funds on their behalf, and distributes them to merchants;
- The program manager, who operates the network and provides services to the issuer (because all program funds are generally maintained in a single account, program managers often maintain the electronic records that track the "movement" of funds into and out of customer's individual wallets);
- The retailer, who sells SVF devices like prepaid cards to customers;
- The network operator, who maintains the link between merchants' point of sale devices, or other payment gateways, and the program manager; and
- Persons, who act as agents for the scheme, such as by accepting cash in exchange for topping up wallet balance.

[5] Please note that one entity can hold various roles related to the provision of SVF (e.g., an issuer of the SVF can also be a program manager). The risk is extended where different agents are involved in the provisioning of a prepaid card.

Another example includes the provision of mobile payment services. The roles of Payment Sector participants depend largely on the business model of the mobile payment service. Furthermore, various roles may be carried out by a single entity or through agents. Entities involved in the provision of mobile payments may include the following:

- The network operator, who provides the platform to allow access to the funds through a mobile phone.
- The distributor (including retailer), who sells or arranges for the issuance of funds on behalf of the issuer to customers.
- The issuer of the SVF, or the electronic money issuer, who issues electronic money, which is defined here as a record of funds or value available to a customer stored on a payment device, such as a prepaid card or mobile phone.

This interplay between different entities can lead to risks resulting from intermediation as discussed above. But it can also give rise to risks when the participating entities have not assigned clear responsibility for compliance with AML/CFT requirements. The PPS risk's exposure may then be dependent on multiple actors who may have a deficient understanding of AML/CFT obligations. For example, in the prepaid card scheme described above agents could facilitate money laundering by accepting large volumes of cash and breaking the value of the deposit up across several wallets, thus avoiding scrutiny related to large cash deposits. The entities acting as merchant acquirers could be aware that the merchants are providing illegal goods or services or are fraudulent, but conceal this knowledge in order to continue to receive fees related to transactions involving the merchants in its network.

The risks created by the use of agents and affiliates increase when agents and affiliates are responsible for sensitive steps in the system (customer or merchant onboarding, or cash acceptance) and when there are multiple agents or affiliates between the customer and the ultimate provider of payment services. For example in card schemes, merchant acquirers will frequently work with contractors who identify merchants and bring them to the acquirer in return for a fee. Depending on the relationships involved, the financial institution that maintains the merchant accounts may not have any actual direct contact with and have a limited visibility of the merchant, as the relationship is intermediated through the merchant acquirer and also the merchant acquirer's contractor. Since contractors do not get paid unless the financial institution accepts the merchant as a customer, they may be incentivized to help the merchant conceal the true nature of its business.

2.1.8. Merchant Risks

All merchants accept payments in one form or another, and most merchants today are at least considering integrating NPPS into their financial arrangements. On the other end of the spectrum, NPPS lower the barriers for merchants to access financial services, making it easier to start and operate a small business, particularly in the e-commerce sector. These lower barriers to entry however can also create risks when merchants are not properly vetted. Globally, Payment Sector participants including providers of NPPS have been abused by or directly complicit with merchants who offer fraudulent or illegal goods or services, or whose business models pose reputational risks to financial institutions. These can for example include traffickers in narcotics who disguise their transactions as financial activity related to a supposedly legitimate small business. They can also include businesses that are legal in some jurisdictions but not others (such as gambling websites) and seek to accept payments from customers resident in jurisdictions where the business is illegal. Finally, they may include sites that are legal in many jurisdictions but that pose

reputational risk, and that are therefore outside a financial institution's risk appetite, or online marketplaces that do not thoroughly police their merchants and thus could themselves be abused by illicit actors.

Any factors—particularly intermediation, nesting, and the use of agents and affiliates—that prevent a financial institution from understanding exactly what merchants or what types of merchants it is serving when it provides a PPS, increase the risks. Risks may be higher in cross-border networks, as businesses may be legal in some jurisdictions and illegal in others, while customers can use the PPS to purchase services that would be illegal in their jurisdiction. Relying on third parties to conduct customer due diligence (CDD) on merchants can also increase risk if the relationship is not well-governed.

2.2. ML/FT Risks for LFIs Providing Services to Payment Sector participants

Many traditional LFIs, including banks, are full participants in the Payment Sector. Banks serve for example as issuers and acquirers in credit, debit, and prepaid card schemes, and are actively involved in developing new payment methods to better serve their customers. When banks play such roles, they are directly exposed to the determinants of risk discussed in section 2.1 above, and should thus conduct appropriate CDD on all Payment Sector participants. Banks and any other LFIs that offer services to other Payment Sector participants, or have customers who use these services, are exposed to specific forms of risk that include:

2.2.1. Correspondent and Correspondent-Type Risk

Because large-scale national clearing and settlement systems are often opened only to banks and other depository institutions, the majority of retail payments will ultimately pass through a bank generally as part of batch settlement. In order to facilitate this activity, non-bank financial institutions involved in payments, as well as unregulated Payment Sector participants, generally maintain deposit accounts with banks. These accounts can be used to safeguard customer funds (for example funds that have been deposited with a prepaid scheme) or to aggregate customer funds before disbursing them directly to customer's account (for example when a merchant acquirer aggregates multiple payments to a merchant partner before disbursing them in a single transfer). Correspondent Banking Relationships in which the correspondent's customers' funds flow through an account held at the respondent financial institution are particularly high risk, because they expose the respondent institution directly to any potentially illicit activity in which the correspondent's customers are engaged. Because banks that offer services to correspondents have limited information on these transactions, they are reliant on the correspondent to implement an effective AML/CFT program. Please see section 3.4.2 for the respective preventive measures.

2.2.2. Other Risks Related to Intermediation

Even banks that view themselves as having limited to no exposure to NPPS may in fact have indirect exposure through customers who link their bank accounts to payment apps, or use their bank accounts to fund SVF accounts or wallets (or withdraw funds received in such wallets to their accounts), or withdraw funds as cash and use it to purchase other prepaid instruments. Account activity of this type poses unique challenges for account and customer surveillance, because frequently the bank will be aware only of the immediate source or destination for the transaction, rather than the entire transaction chain. This can allow customers to deliberately thwart transaction monitoring programs and prevent the bank from understanding and assessing the activity on the customer's account to determine whether it is in fact in line with the

customer profile. Examples of how intermediation can limit a bank's ability to identify suspicious or unusual behavior include:

- Many banks have automated transaction rules designed to identify possible unlicensed money transfer activity by alerting on accounts that receive multiple small deposits from different sources, followed by a single large cross-border transaction. A customer could thwart this surveillance by having associates deposit the funds to be transferred in an SVF wallet, and then moving those funds to a linked bank account in order to execute the cross-border transfer. From the bank's perspective, it would appear that the customer received only one deposit. Relatedly, the provider of SVF could not know that the funds were ultimately transferred across borders.
- Many banks use watchlists to identify transactions that may be illegal or in violation of bank policy, such as the use of gambling websites. A customer seeking to evade these restrictions could use a foreign payment app linked to their account to purchase the assets; this transfer would likely appear on the bank's records as a debit in favor of the operator of the payment app. The operator, in turn, may not be responsible for enforcing the laws of the jurisdictions where its foreign customers are based. It is therefore important for banks to identify foreign payment apps in order to appropriately assess the risks of the transactional activity.
- A customer that generates a high quantity of illicit proceeds in cash can evade surveillance the bank applies to cash deposits by depositing the cash with a provider of NPPS (including both SVF and any other payment app that accepts cash inputs) and then withdrawing the funds from the payment service to his/her linked bank account.

2.2.3. Risks Related to Outsourcing

Banks often serve as the backbones of PPS such as credit, debit, and prepaid schemes without serving as the administrator or governing body of the scheme. In these situations, banks provide their reputation, stability, ability to hold deposits, and access to national payment systems while program administrators actually manage the movement of funds throughout the scheme. Because program operators have more direct contact with customers and more insights into the movement of funds, banks involved in these schemes often outsource CDD and other elements of the AML/CFT program to the program operators**.** But **as banks continue to be exposed to funds involved in the program, they remain responsible for implementing an effective and compliant AML/CFT program, even if transactions flow through third parties** that may or may not be subject to AML/CFT requirements. LFIs should therefore adopt policies to mitigate risks arising from reliance on outside service providers, including ones that operate in high-risk countries. Where roles and responsibilities are not clearly assigned, or where the program administrator does not implement an effective program, illicit actors can exploit the cracks in the program, and the bank and the program operator together will likely be less effective than if either party were operating alone. In such cases, LFIs should maintain a contingency arrangement as necessary.

3. Mitigating Risks

LFIs, whether they are primarily Payment Sector participants or have more limited exposure, are expected to take a risk-based approach to mitigating and managing ML/FT risks related to this sector, including the risks arising from the use of NPPS. A risk-based approach means that risk mitigation should begin with, and be based on, an appropriate assessment of the LFI's payments-related risks. This assessment should in turn be reflected in the design and operation of the LFI's AML/CFT program, including but not limited to

the particular program elements discussed below, so that the LFI devotes greater resources and attention where risks are higher.

The sections below discuss how LFIs can apply specific preventive measures to mitigate and manage their payments-related risk. Sections 3.1-2 and 3.5-7 apply to all LFIs. Section 3.3 describes preventive measures recommended for LFIs that provide PPS directly to customers (including both consumers and merchants, or payers and payees), and section 3.4 for LFIs that provide services to other Payment Sector participants. The controls discussed should be integrated into the LFI's larger AML/CFT compliance program and supported with appropriate governance and training. It is not an exhaustive discussion of all AML/CFT requirements and LFIs should continuously consult the UAE legal and regulatory framework currently in force.

3.1. AML/CFT obligations under CBUAE Regulations

The CBUAE regulatory framework clearly state expectations for compliance with AML/CFT obligations. In addition to this guidance, LFIs including non-bank payment service providers should carefully review all the relevant regulations issued by the CBUAE, which provide a comprehensive coverage of all payment products, services, and systems that are issued, provided and/or operated in the UAE, to ensure they fully understand and comply with their obligations.

3.1.1. Providers of Stored Value Facilities

In November 2020 the CBUAE issued the *Stored Value Facilities (SVF) Regulation* (Circular No. 6/2020 issued by Notice 4834/2020). Under its Article 14, all licensees must comply with the existing legal obligations and regulatory requirements for AML/CFT of the CBUAE and address ML/FT risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, detect ML/FT activities, and report any suspicious transactions to the UAE Financial intelligence Unit (UAE FIU). Among their detailed regulatory obligations, the licensees must assess the risk level of business relationships and undertake periodic risk profiling and assessment of products based on the AML/CFT requirements.

3.1.2. Retail Payment Services and Card Schemes Regulation

In July 2021 the CBUAE issued the *Retail Payment Services and Card Schemes Regulation* (Circular No. 15/2021 issued by Notice 3603/2021). Under its Article 12, payment service providers must comply with the relevant UAE AML/CFT laws and regulations and address ML/FT risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, detect ML/FT activities, and report any suspicious transactions to the UAE FIU. Among their detailed regulatory obligations, the licensees must conduct business relationship-specific risk assessments and undertake periodic risk profiling and assessment of retail payment service users based on AML/CFT requirements. In addition, under Article 18.14, card schemes must report transactions to the UAE FIU when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime.

3.1.3. Large Value and Retail Payment Systems Regulations

In March 2021 the CBUAE issued the *Large Value Payment Systems Regulation* (Circular No 9/2020 issued by Notice 1410/2021) which covers clearing and settlement systems designated primarily to process large-value and/or wholesale payments typically among financial market participants or involving money market, foreign exchange or many commercial transactions. In tandem, the CBUAE issued the *Retail Payment*

Systems Regulation (Circular No. 10/2020 issued by Notice 1408/2021) which covers fund transfer systems and related instruments, mechanisms, and arrangements that typically handle a large volume of relatively low-value payments in such forms as cheques, credit transfers, direct debit, card payment transactions or a regulated medium of exchange. Among their detailed regulatory obligations, all licensees are required to comply with any instructions issued by the CBUAE and any relevant international standards.

3.2. Risk Assessment

Under Article 4 of the AML-CFT Decision, LFIs are required to identify, assess, and understand the ML/FT risks to which they are exposed and how they may be affected by those risks, in order to determine the nature and extent of AML/CFT resources necessary to mitigate and manage those risks. In addition, under Article 23 of the Decision, LFIs are required to identify and assess the ML/FT risks of that may arise when developing new products and new professional practices, including means of providing new services and using new or under-development techniques for both new and existing products. **An appropriate risk assessment should consider all the PPS that an LFI provides, and the LFI's direct relationships to Payment Sector participants, both domestic and foreign.**

When assessing its direct exposure to the Payment Sector, whether in the form of PPS it offers, or relationships it maintains with other participants, the LFI should consider the risk factors discussed in section 2 above. The risk assessment should take into consideration:

- **Movement of Funds.** What are the financial flows through the PPS and through the LFI's accounts? What is the speed of transactions? Is there a cap on transaction value? Is there a daily, weekly, or monthly cap on the volume of transactions? Is the payment service in question closed loop or open loop? Can single users open multiple accounts?
- **Mode of Funding:** How do users fund their accounts and make withdrawals, and is funding permitted prior to customer verification?
- **Peer-to-Peer Payments.** Does the PPS allow users to conduct peer-to-peer transfers, or can they only send transfers to merchants/from customers? How is this restriction implemented and enforced?
- **Cross-Border Movement.** Does the PPS permit funds to move across borders and to high-risk countries through relationships with foreign financial institutions? Can users access the PPS when they are outside the UAE? Does the service support multiple currencies?
- **Regulatory Status.** Is the PPS that the LFI provides a regulated activity in the UAE and in all jurisdictions where it is provided?
- **Use of Agents and Affiliates**. How many entities are involved in delivering the PPS? How open is the network supporting the PPS? Does it include entities that are not regulated as LFIs—for example convenience stores that accept cash in return for topping up account balance? What is the role of each player in the system, and are responsibilities clearly defined in governance documents?
- **Intermediation.** How much visibility does the LFI have into payment activity taking place through the PPS? Can the LFI identify the ultimate payer and payee for all transactions? How many entities are in the payment chain?

- **Controls.** Does the PPS integrate appropriate features that contribute to managing the risk created by the factors listed above, such as by performing a robust customer verification process? These can include both the AML/CFT-specific features discussed in section 3.3 below and measures related to cybersecurity and counter-fraud.

Where LFIs, particularly banks, provide services such as deposit accounts to Payment Sector participants, they should also consider the following in assessing the risk of the relationship:

- **Nature of the Relationship:** What products or services does the LFI provide to the participant? Does the relationship involve direct exposure to the funds of the participant's customers? Is the sector participant using the relationship to facilitate activity by other Payment Sector participants?
- **Regulatory Status:** Is the participant required to be licensed in the UAE, its home jurisdiction, and all jurisdictions where it operates? Is it subject to AML/CFT requirements in all jurisdictions that are at least as stringent as those imposed in the UAE?
- **Relationship Governance:** Are AML/CFT responsibilities within the relationship clearly defined? Does the LFI outsource some aspects of AML/CFT program implementation to the Payment Sector participant?

The risk assessment should also consider the LFI's indirect exposure to the Payment Sector through its customers, who may connect their account with an LFI to a variety of PPS, or may fund their account by using such PPS. Because many payment service providers use existing domestic or international payment systems to execute transfers on behalf of their customers, an LFI may not be aware that its customers are using such services nor able to prohibit their use or detect payments activity in customer's accounts. LFIs should therefore consider a variety of tools to assess their indirect exposure to this sector. These may include:

- applying appropriate level of due diligence and asking questions during the CDD process to obtain all relevant information;
- administering customer surveys to better understand customer's interest in and use of payment services; and
- utilizing watchlist-based screening over a sample period.

When LFIs have a sense of the most common PPS their customers use, they should assess the risk these services and products pose, considering the factors discussed above, including the involvement of high-risk countries and the extent of exposure. 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.

3.3. Preventive Measures for LFIs Providing Products and Services directly to Customers

Under Article 4(2) of the AML-CFT Decision, all LFIs must implement an AML/CFT program designed to manage the risks identified in their risk assessment that should include:

3.3.1. Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring

Under Article 5 of the 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. Payment Sector participants, including providers of SVF, retail payment services, and card schemes, generally establish relationships with their customers rather than treat all customers as occasional or walk-in customers. In these scenarios, **LFIs must perform, no matter the customer type, all the elements of CDD required under sections 2 and 3 of the AML-CFT Decision**, which include customer identification and verification, beneficial owner identification, understanding of the nature of the customer's business and purpose of the business relationship, and ongoing monitoring. CDD, and where necessary enhanced due diligence (EDD), are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers.

In addition to these mandatory elements, LFIs should consider the following additional elements of CDD that are particularly important in the context of NPPS:

- **User identification and verification.** Many, if not most, NPPS involve the use of digital as opposed to face-to-face methods of onboarding and identifying customers (a.k.a. "electronic Know Your Customer," or "e-KYC"). Digital delivery of services is increasingly common, but can present higher risks when LFIs do not take appropriate steps to ensure that they fully understand the customer and that the person using the services is in fact the identified customer. In particular, when verifying the Emirates ID card (either physically or by way of digital or e-KYC solutions) LFIs must use the online validation gateway of the Federal Authority for Identity, Citizenship, Customs & Port Security, the UAE-Pass Application, or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where passports, other than the Emirates ID are used in the KYC process, a copy must be physically obtained from the original passport which must be certified (i.e. certified copy) as "Original Sighted and Verified" under the signature of the employee who carries out the CDD process and retained.
- **Use of IP addresses and geographical (spatial and temporal) locators**. As discussed above, payment services that are internet-based or accessible through smartphones can allow customers to access financial services no matter where they are in the world. LFIs are of course free to allow their customers to access their services while outside the UAE, but should take advantage of geographical location tools at both the onboarding and the ongoing monitoring stages to ensure that they understand the geographic risk they might be exposed to by their customers. This can include:
    - Requiring additional authentication or verification when a customer accesses the service from an IP address or device different from the one used at onboarding, or from a different country and/or time zone than the customer's stated country of residence.
    - Reviewing the customer's log-in locations during CDD refresh to identify any suspicious log-in or movement patterns (for example, high numbers of transactions taking place when the customer is near a border with a high-risk country where the PPS is blocked).
- **SVF due diligence**: Risk mitigating measures should include as per Article 14.4 of the SVF Regulation: (a) the application of limits on the maximum storage values, cumulative turnover or transaction amounts; (b) disallowing higher risk funding sources; (c) restricting the SVF product being used for higher risk activities; (d) restricting higher risk functions such as cash access; and

(e) implementing measures to detect multiple SVF accounts/cards held by the same Customer or group of Customers.

- **Merchant due diligence.** Payment Sector participants that deal directly with merchants (whether as providers of SVF or card schemes, or conducting merchant acquisition or payment aggregation) may have two main classes of customers: consumers and merchants. It is important to remember that merchants who use the service are customers of the LFI and that merchants that may engage in deceptive or fraudulent business practices or use their legitimate business as a cover for criminal activities, can expose the LFI to extremely high ML/FT risk. Merchants should therefore be subject to CDD designed to understand the nature of their business and the expected transaction volumes. LFIs should understand the merchant's current financial and payments operations and in particular ascertain why the merchant is seeking a new provider of financial services, as fraudulent merchants may move from LFI to LFI seeking to conceal their activities**.** Merchants operating in higher-risk sectors, and those that are cash-intensive businesses, are likely to require EDD that could involve performing a periodic site visit of the merchant's place of business. For more information, please consult the CBUAE's *Guidance for LFIs providing services to the Real Estate and Precious Metals and Stones sectors,* and *Guidance for LFIs providing services to Cash-Intensive Businesses*.

As per Article 7 of the AML-CFT Decision, all customers must be subject to ongoing monitoring to make sure that CDD information on file is accurate, complete and up-to-date and to ensure that transactions conducted are consistent with the expected customer profile. To support this process, LFIs should apply solutions that ensure the accuracy and completeness of their data. It also may be appropriate to include non-standard elements of monitoring to reflect the risks of payments customers, such as geographic and IP-address monitoring discussed above, and the monitoring of the balance between peer-to-peer and merchant payments in a customer's account. For merchant relationships, ongoing monitoring should include an examination of the number of 'chargebacks' or refunds the LFI has had to award to customers of the merchant, as well as any customer complaints the LFI has received. Where a merchant generates a large number of customer complaints or refund requests, or none at all, it may be a sign that it is operating a fraudulent business.

3.3.2. Controls

In line with their risk appetite and AML/CFT program, LFIs should develop controls that are commensurate with the nature and size of their business to enable them to manage the risks identified. Effective controls are those designed to minimize or eliminate those aspects of the PPS and NPPS that make them most attractive to illicit actors as discussed in section 2 above. LFIs should in particular consider:

- **Geographical limits.** LFIs should strongly consider using IP addresses and smartphone geolocation capabilities to prevent customers accessing PPS from high-risk countries. 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)[6], the UAE Financial Intelligence Unit (UAE FIU), and the FATF. LFIs may also use public free databases such as, for example, the Basel AML Index[7] or the Transparency International Corruption Perceptions Index.[8] LFIs should not solely rely on public lists, however, and should consider their

[6] Available at: https://www.namlcftc.gov.ae/en/more/jurisdictions/
[7] Available at: https://baselgovernance.org/basel-aml-index
[8] Available at: https://www.transparency.org/en/cpi/2020/index/nzl

own experiences and the nature of their exposure to each jurisdiction when assessing the risk of that jurisdiction. LFIs should be aware, however, that given the widespread availability of Virtual Private Network (VPN) services, simply using IP address-based screening is not likely to be effective in preventing access to their service from specified areas. LFIs that use this control should make sure their systems are designed to detect VPN usage.

- **Transaction limits.** Smaller transactions are not without illicit finance risk, but from the perspective of materiality, transaction and volume limits (daily, weekly, monthly, etc.) can decrease an LFI's exposure to illicit payments and also make the PPS overall less attractive to illicit actors.
- **Funding constraints.** Requiring customers to fund their accounts and to withdraw funds using only transfers from regulated domestic financial institutions can help protect PPS from the risks related to cash and ensure that the customer will be subject to CDD and monitoring.
- **Multi-factor authentication.** Requiring customers to provide a One-Time Password (OTP), or answer a phone call, or prompt on their smartphone when logging into an internet-based PPS can help prevent the misappropriation of customer funds by hackers. With regard to the OTP, all banks are required to include specific information in the messages that contain an OTP (full transaction amount, detailed beneficiary merchant name and website and a dedicated telephone number for customers to report suspected fraudulent activity). Banks are also required to ensure that card acquirers and issuers assist them to provide the additional OTP information as needed.[9]

3.3.3. Wire Transfers requirements

Articles 27-29 of the AML-CFT Decision contain specific requirements with regard to information that LFIs must collect, and transmit with the wire transfer, when conducting an international wire transfers as well as specific obligations related to domestic wire transfers. In addition, Guidance on CDD measures concerning wire transfers is laid down in section 6.3.2 of the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions.* It is important to note that since many Payment Sector participants qualify as financial institutions, the applicability of these requirements is wide-ranging.

3.4. Preventive measures for LFIs Providing Services to other Payment Sector participants

3.4.1. Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring

As mentioned above, LFIs must conduct appropriate CDD on all customers, regardless of their type or sector. The majority, if not all, of Payment Sector participant customers will be legal persons for which LFIs should conduct CDD as required by Articles 8 and 9 of the AML-CFT Decision. In particular, under Article 9 of the AML-CFT Decision, LFIs are required 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, and where no such individual meets this description, the LFI must identify and verify the identity of the relevant individual(s) holding the senior management position in the entity. For more information, please consult the CBUAE's *Guidance for Licensed Financial Institutions providing services to Legal Persons and Arrangements*. LFIs should ensure that their

[9] Notice 4892/2021 issued by the CBUAE to all Banks in October 2021 regarding *"One-Time Password (OTP) for card transactions".*

contractual agreements with Payment Sector participant customers ensure that the LFI can access necessary information in a timely fashion. **If LFIs cannot access this information in accordance with timelines laid out in its policies, they should consider restricting and ultimately terminating the relationship**.

Furthermore, as per Articles 8.3 and 4 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 expected uses to which the customer will put the LFI's products and services. In the context of payments, the LFI must understand whether and how its services are being used by its Payment Sector participant customer to facilitate provision of the PPS to its customer (Payment Sector participant customers may also be transacting on a proprietary basis). This should include a determination of whether nesting will take place. If the LFI prohibits nesting, it should make that prohibition clear to the customer.

In addition to the standard required CDD elements of Sections 2 and 3 of the AML-CFT Decision, LFIs should collect all the information necessary to risk-rate the Payment Sector participant customer considering the risk factors described in section 3.2 above and whether aspects of the customer profile require EDD. LFIs should also consider the following steps to gain a more detailed understanding of the customer's business in order to be sure that they fully understand it:

- Review the customer's promotional materials, including its website, to understand its target customers and the services it purports to offer.
- Understand how the customer provides payment services, the other participants it works with to do so, and whether it uses agents or affiliates.
- Requiring the customer to identify its major merchant customers by providing information such as the merchant's name, principal business activity, geographic location, and transaction volume, and use public records searches or information provided by the customer to determine whether these merchants are operating a legitimate business.
- Visiting the customer's headquarters and business operations center and evaluating the customer's AML/CFT controls.
- Reviewing public databases to ensure that the customer, its beneficial owners, and its senior management have not been subject to law enforcement actions.

Under Article 7 of the AML-CFT Decision, all customers must also be subject to ongoing monitoring throughout the business relationship. Changes in the design or structure of a PPS, as well as changes in a Payment Sector participant's customer base (including both the consumer and merchant customer base), can have a major impact on the overall risk associated with the Payment Sector participant. Ongoing monitoring of the customer relationship should be sufficiently rigorous to identify when such changes have taken place, as well as any other changes that impact the customer's risk rating, and should be conducted at a frequency appropriate to the customer's risk and the materiality of its transactions. Ongoing monitoring should also include a review of the customer's transactional activity to determine whether it is in line with expectations established at onboarding and with activity during the previous review period. Sharp or substantial changes in activity may have a fully legitimate cause, such as growth in the customer's user base, but LFIs should still ensure they understand the reasons for these changes.

3.4.2. Correspondent Due Diligence

Article 25 of the AML-CFT Decision sets out specific mandatory requirements for LFIs entering into a Correspondent Banking Relationship or any similar relationship, no matter the nature of their customer, which include the following:

- Refrain from entering into or maintaining a Correspondent Banking Relationship with shell banks or an institution that allows their accounts to be used by shell banks;
- Collect sufficient information about any receiving correspondent banking institution for the purpose of identifying and achieving a full understanding of the nature of its business and to make available, trough publicly available information, its reputation and level of control, including whether it has been investigated;
- Evaluate the AML/CFT controls applied by the receiving institution;
- Obtain approval from senior management before establishing new Correspondent Banking Relationship; and
- Understand each institution's AML/CFT responsibilities.

In the context of Correspondent Banking Relationships with Payment Sector participants, LFIs should conduct correspondent due diligence that reflects the unique risks and features of those relationships. As discussed above, in the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, **each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it.** Thus, LFIs should be aware of intermediated risk posed by Payment Sector participants—including providers of SVF, retail payment services, and card schemes—that access banking services through their accounts with an LFI. As a result, LFIs should in particular consider:

- **Regulatory status**. As discussed above in section 2.1.4, jurisdictions take different approaches to regulating the Payment Sector, and not all Payment Sector participants that would qualify as financial institutions under the UAE's legal and regulatory framework are required to be licensed and regulated in their home jurisdiction. When offering services to a foreign entity, LFIs should consider not just its licensing status under its home jurisdiction's laws, but its licensing status should it carry out those same activities in the UAE. Where a foreign entity would require a license in the UAE, LFIs should treat it as a financial institution and subject it to correspondent due diligence. In these cases, LFIs should be particularly cautious to ensure that their correspondent implements an AML/CFT program that at least meets the requirements of the AML-CFT Law and Decision, and be aware that the correspondent is likely not supervised to ensure effective implementation of this program, increasing its risk.
- **Merchant Due Diligence.** LFIs should ensure that their Payment Sector participant customers conduct appropriate due diligence not just on customers but on merchants as well. LFIs should request and review the correspondent's due diligence policies, procedures, and processes to determine the adequacy of its due diligence standards for merchant and consumer customers.
- **Controls related to nesting.** When an LFI offers services to a correspondent without knowing that nesting is taking place, it is unable to take appropriate measures to manage the risk of the nested relationship and, thus, likely to be exposed to higher risks. LFIs should therefore always understand

all purposes for which the correspondent account will be used and ensure that the CDD and monitoring applied to the relationship will assess whether nesting is taking place.

- **Testing and auditing.** On a risk-basis, LFIs should consider taking active measures to test the correspondent's AML/CFT program. This can include, at a minimum, reviewing the correspondent's internal audit reports and can extend to requiring the correspondent to hire an external auditor, conducting on-site reviews and discussions at the correspondent's premises.

3.5. Targeted Financial Sanctions

Article 16.1 of the AML-CFT Law and Article 60 of the AML-CFT Decision require LFIs to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations. In furtherance of this requirement, the Cabinet Decision 74 of 2020 sets out the legal and regulatory framework in the UAE regarding Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List. For more information, please consult the Executive Office of the Committee for Goods and Material Subjected to Import and Export Control's *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions and Virtual Assets Service Providers*[10], the CBUAE's *Guidance for LFIs on the Implementation of TFS,* and *Guidance for LFIs on Transaction monitoring and Sanctions screening*[11].

LFIs should take appropriate steps to develop, implement and regularly update an appropriate Sanctions Compliance Program in order to fulfil their obligation to comply with the related requirements that includes screening of customers and transactions. LFIs should be aware that, for all PPS they offer, they should have in place operational systems that ensure they can appropriately screen transactions related to those products or services. If they cannot conduct appropriate screening, they should not offer that product or service. **LFIs should also ensure that the required information fields are created and duly transmitted throughout the payment cycle across the different PPS**. LFIs should screen all information they have about a transaction, including any messages between users engaging in a peer-to-peer transfer that may have a non-uniform number of characters, use special characters, or present other challenges to screening systems.

An LFI that does not wish to have any exposure to high-risk countries will need to take additional measures to control where its customers use its products or services. Furthermore, sanctions risk assessments can change from time to time depending on where a customer is currently located. In intermediated correspondent relationships, LFIs should ensure that they fully understand their correspondents' sanctions screening approaches, and **should not process any payments for a correspondent unless they are entirely confident that the correspondent conducts appropriate screening**. LFIs cannot rely on another LFI to fulfill screening obligations related to transactions on their own accounts or systems.

Furthermore, LFIs must sign up for the Integrated Enquiries Management System ("IEMS") introduced by the UAE FIU to automate and facilitate the execution process of requests for information, implementing decisions of public prosecutions and any other type of ML/FT requests. Via this system, the FIU can make requests to all LFIs simultaneously with the goal of processing requests and providing results to law enforcement authorities more efficiently. For more information, please consult the *IEMS User Guide* published by the UAE FIU.[12]

[10] Available at https://www.uaeiec.gov.ae/en-us/un-page#
[11] Available at https://www.centralbank.ae/en/cbuae-amlcft
[12] Available at https://www.uaefiu.gov.ae/media/jtdnttby/integrated-enquiry-management-system.pdf

3.6. Transaction Monitoring and Suspicious Transaction Reporting

Under Article 16 of the 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), a Suspicious Activity report (SAR) or other report types. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/FT risks of the institution's customers, products and services, delivery channels, and geographic exposure. For more information, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening*.

As required by Article 15 of the AML-CFT Law and Article 17 of the AML-CFT Decision, LFIs must file a STR, a SAR or other report types with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, is related to a crime, or is 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. By filing STRs with the UAE FIU, LFIs alert law enforcement authorities about suspicious behaviour and allow investigators to piece together transactions occurring across multiple LFIs.

As discussed above, in the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, **each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it.** Although LFIs cannot outsource their responsibility to report suspicious activity, they can outsource certain aspects of transaction monitoring. In the prepaid card scheme described in section 2.1.7, for example, the bank that offers the prepaid cards may outsource automated transaction monitoring to the program manager, which has more direct insight into individual transactions. The bank in this situation, and any LFI that outsources any elements of transaction monitoring, nevertheless retains ultimate responsibility for identifying and reporting suspicious transactions.

3.7. 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. Therefore, in addition to the mandatory governance and training requirements set forth in the AML-CFT Law and Decision, Payment Sector participants and LFIs providing them services should endeavor to incorporate the following considerations into the design of their governance frameworks and their training programs.

- **Clear allocation of AML/CFT responsibilities among LFIs.** When a network of Payment Sector participants combine to deliver a payment service and execute transactions, risks arise when they do not have a clear understanding of each participant's AML/CFT responsibilities. Allocating responsibilities is particularly important when some LFIs involved in a payment will not form a relationship with the ultimate customer or beneficiary. Card schemes should have a governing body, but this may not be a requirement for other Payment Sector participants depending on their role in processing payments. LFIs should understand the parties and their roles and responsibilities in the scheme and manage risks accordingly. **Any LFI that provides payment services as part of a network should assume full responsibility for CDD**. Furthermore, LFIs cannot rely on any other entities to implement elements of the AML/CFT program, such as the appointment of a compliance officer and the reporting suspicious transactions. **Similarly, when a LFI provides**

services to a Payment Sector participant as part of a Correspondent Banking Relationship, they should also understand each party's AML/CFT responsibilities and document them in the contract or other program documents. Understanding the parties' respective AML/CFT responsibilities is a mandatory element of correspondent CDD under Article 25 of the AML-CFT Decision.

- **Agent Governance and Training.** Where a payment service or product relies on the use of agents for delivery, it is critical that they are appropriately trained to recognize red flags for illicit activity, and to carry out the elements of the AML/CFT program for which they are responsible. LFIs that use agents should have appropriate programs in place to manage them through effective governance arrangements that, among other measures, set clear requirements for terminating relationships if agents do not comply with the LFI's policy. LFIs should provide training directly to agents and test their compliance on a regular basis. Where agents participate in sensitive activities, such as cash acceptance or onboarding, they should receive increased training and be subject to additional controls and testing.
- **Employee Training.** 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 PPS, 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 Payment Sector participants that offer PPS as their primary business, employee training should be focused on payments-related risks. For LFIs that offer services to Payment Sector participants, employee training should cover payment risks as appropriate to the employee's role and responsibilities as well as the LFI's overall exposure to the sector.

Annex 1. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding and effective performance by Licensed Financial Institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.
	Applicability	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, stored value facilities, retail payment service providers, and card schemes.
Understanding Risks	ML/FT Risks of the Payment Sector	**Characteristics of the Movement of Funds**: Products and Services (PPS) and New Payment Products and Services (NPPS)in particular are extremely attractive to illicit actors because of the rapid movement of funds between Payment Sector participants and across borders. The risks vary based on transaction speed, transaction limits, closed vs. open loop system, methods of funding and access to cash, payment transparency, ability for one person to create multiple accounts, non-face-to-face relationships, and use of virtual assets (the latter is addressed in a separate guidance to be issued by CBUAE).
		Peer-to-Peer Payments: NPPS allow participants to send money that will be instantly available to the beneficiary, reducing the need for trust in the relationship. The use of PPS for peer-to-peer payments creates risk for financial institutions because transactions can flow through third parties that may not be subject to AML/CFT requirements.
		Cross-Border Movement: Many NPPS can be used globally for making payments or transferring funds, thus introducing banks to new geographical exposure. Unlike cross-border wires, which carry full identifying information, banks will frequently only see the customer's transactions with the payment network itself, rather than their location or ultimate destination.
		Global Regulatory Gaps: Countries take a variety of approaches to regulating the Payment Sector and there is no one widely accepted classification of participants. And participants, as relatively new market entrants, may lack the experience, expertise, or commitment to apply fully effective preventive measures.
		Intermediation: A number of participants potentially involved in a single transaction. Intermediated transactions create risk because no regulated entity participating in the transaction has the visibility necessary to fully understand the transaction and the participants.
		Nesting: Nesting is a form of intermediation that presents specific risks. In most Correspondent Banking Relationships that involve nesting, the respondent financial institution is not aware of individual transactions ordered by the ultimate customer.
		Use of Agents and Affiliates: Payment Sector participants often interact in a dense web of agency and affiliate relationships. A large number of entities involved in the NPPS, in particular when involving several countries, may increase the ML/FT risk. The interplay between different entities can lead to risks from intermediation and also when the participating entities have not assigned clear responsibility for compliance with AML/CFT requirements.
		Merchant Risks: Globally, Payment Sector participants including providers of NPPS have been abused by or directly complicit with merchants who offer fraudulent or illegal goods or services, or whose business models pose reputational risks to financial institutions. Relying on third parties to conduct customer due diligence (CDD) on merchants can also increase risk if the relationship is not well-governed.

Understanding Risks	ML/FT Risks for LFIs Providing Services to Payment Sector Participants	**Correspondent and Correspondent-Type Risk:** Correspondent Banking Relationships in which the correspondent's customers' funds flow through an account held at the respondent financial institution are particularly high risk, because they expose the respondent institution directly to any potentially illicit activity in which the correspondent's customers are engaged. Because banks that offer services to correspondents have limited information on these transactions, they are reliant on the correspondent to implement an effective AML/CFT program.
		Other Risks Related to Intermediation: Even banks that view themselves as having limited to no exposure to NPPS may have indirect exposure through customers who link their bank accounts to payment apps, or use their bank accounts to fund stored value facilities (SVF) accounts or wallets, or withdraw funds as cash and use it to purchase other prepaid instruments.
		Risks Related to Outsourcing: Banks often serve as the backbones of PPS such as credit, debit, and prepaid schemes without serving as the administrator or governing body of the scheme. Banks involved in these schemes often outsource CDD and other elements of the AML/CFT program to the program operators who have more direct contact with customers and insight to movement of funds. But Banks remain responsible for implementing an effective and compliant AML/CFT program.
Mitigating Risks	AML/CFT obligations under CBUAE Regulations	In addition to this guidance, LFIs including non-bank payment service providers should carefully review all the relevant regulations issued by the CBUAE, which provide a comprehensive coverage of all payment products, services, and systems that are issued, provided and/or operated in the UAE, to ensure they fully understand and comply with their AML/CFT obligations. In 2020-2021 the CBUAE issued the SVF Regulation, the Retail Payment Services and Card Schemes Regulation, the Large Value Payment Systems Regulation, and the Retail Payment Systems Regulation.
	Risk Assessment	An appropriate risk assessment should consider all the PPS that an LFI provides, and the LFI's direct relationships to Payment Sector participants, both domestic and foreign. When assessing an LFI's direct exposure to the Payment Sector, the LFI should consider the risk factors discussed in section 2 of the Guidance, such as the movement of funds, mode of funding, and peer-to-peer payments among others. Where LFIs provide services to Payment Sector participants, they should also assess the risk of the relationship as well as their indirect exposure to the Payment Sector through their customers.
	Preventive Measures for LFIs Providing Products and Services directly to Customers	**Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring**: LFIs must perform all the elements of CDD, which include customer identification and verification, beneficial owner identification, understanding of the nature of the customer's business and purpose of the relationship, and ongoing monitoring. In addition to these mandatory elements, LFIs should consider the following elements that are particularly important in the context of NPPS: user identification and verification, use of IP addresses and geographical (spatial and temporal) locators, and SVF and merchant due diligence.
		Controls: LFIs should develop controls that are commensurate with the nature and size of their business to manage the risks identified. LFIs should in particular consider geographical limits, transaction limits, funding constraints, and multi-factor authentication to minimize or eliminate those aspects of the PPS and NPPS that make them most attractive to illicit actors.
		Wire Transfers Requirements: The AML-CFT Decision contain specific requirements with regard to information that LFIs must collect, and transmit with the wire transfer, when conducting an international wire transfers as well as specific obligations related to domestic wire transfers (the Guidelines further contain CDD measures). Since many Payment Sector participants qualify as financial institutions, the applicability of these requirements is wide-ranging.

Mitigating Risks	Preventive Measures for LFIs Providing Services to other Payment Sector Participants	**Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring**: LFIs must conduct appropriate CDD on all customers, regardless of their type or sector (the majority, if not all, of Payment Sector participant customers will be legal persons). In this context, the LFIs should also consider a determination of whether nesting will take place. In addition to the standard required CDD elements, LFIs should collect all the information necessary to risk-rate the Payment Sector participant customer and evaluate whether aspects of the customer profile require EDD. All customers must also be subject to ongoing monitoring throughout the business relationship.
		Correspondent Due Diligence: In the context of Correspondent Banking Relationships with Payment Sector participants, LFIs should conduct correspondent due diligence that reflects the unique risks and features of those relationships. In the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it. LFIs should in particular consider regulatory status, merchant due diligence, controls relating to nesting, and testing and auditing of the correspondent's AML/CFT program.
	Targeted Financial Sanctions	LFIs are required to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations and the requirements set by Cabinet Decision 74 of 2020 regarding Targeted Financial Sanctions. LFIs should be aware that, for all PPS they offer, they should have in place operational systems that ensure they can appropriately screen transactions related to those products or services. In intermediated correspondent relationships, LFIs should ensure that they fully understand their correspondents' sanctions screening approaches, and should not process any payments for a correspondent unless they are entirely confident that the correspondent conducts appropriate screening.
	Transaction Monitoring and Suspicious Transaction Reporting	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), a Suspicious Activity report (SAR), or other report types. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD. As discussed above, in the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it. Any LFI that outsources any elements of transaction monitoring retains ultimate responsibility for identifying and reporting suspicious transactions.
	Governance and Training	Payment Sector participants and LFIs providing them services should endeavor to incorporate the following considerations into the design of their governance frameworks and their training programs: clear allocation of AML/CFT responsibilities among LFIs, agent governance and training, and employee training. When a network of Payment Sector participants combine to deliver a payment service and execute transactions, risks arise when they do not have a clear understanding of each participant's AML/CFT responsibilities. Any LFI that provides payment services as part of a network should assume full responsibility for CDD. When a LFI provides services to a Payment Sector participant as part of a Correspondent Banking Relationship, they should also understand each party's AML/CFT responsibilities and document them in the contract or other program documents.