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 IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS

July 4, 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*[1] (issued by Notice No. 74/2019 dated 19/06/2019) and the Executive Office of the Committee for Goods and Materials Subject to Import and Export Control's ("Executive Office") *Guidance on Targeted Financial Sanctions for Financial Institutions and Designated Non-financial Business and Professions*[2] (circulated by CBUAE Notice No. 2893 dated 02/06/2021) and any amendments or updates thereof. 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 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.
[2] Available at: https://www.uaeiec.gov.ae/en-us/un-page#

1.3. Legal Basis

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

- Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementation Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions ("Cabinet Decision 74").

The AML-CFT Law and 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 ("UNSC") under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision 74 sets out the legislative and regulatory framework regarding the Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List.

The Executive Office[3] acts as a national lead to coordinate and liaison implementation of TFS with all the federal and local government stakeholders including financial institutions (FIs) and designated non-financial business and professions (DNFBPs) and has issued the *Guidance on Targeted Financial Sanctions for FIs and DNFBPs*". The Executive office is mainly responsible for:

- Receiving and processing grievances against Listing in UN and Local Lists decisions;
- Receiving and processing applications to use frozen funds as per sanctions lists;
- Working closely with the Supreme Council with regards to the local Listing;
- Circulating updates to the local and UN lists to the government and private sector; and
- Coordinating and exchanging information between Government Agencies.

This Guidance issued by the CBUAE is supplementary to the above mentioned "*Guidance on Targeted Financial Sanctions for Financial Institutions and Designated Non-financial Business and Professions*" issued by the Executive Office.

1.4. Definitions

Controlling Shareholder: A shareholder who has the ability to directly or indirectly influence or control the appointment of the majority of the board of directors, or the decisions made by the board or by the general

[3] Website: Home | Committee for goods & material subjected to import & export (uaeiec.gov.ae)

assembly of the entity, through the ownership of a percentage of the shares or stocks or under an agreement or other arrangement providing for such influence.

Direct Relationship: A relationship between two parties that knowingly provide the other material, technological, logistical, or financial support and both parties are directly impacted by the other party.

Funds: Assets of all types, in whatever form and however acquired, whether corporeal or incorporeal, tangible or intangible, movable or immovable, electronic, digital or encrypted, including national currency, foreign currencies, documents and legal instruments establishing ownership of such assets or any associated rights, in whatever form, including electronic or digital forms, as well as economic resources considered as assets of any kind, including oil and natural resources, and bank credits, cheques, money orders, shares, securities, bonds, drafts, and letters of credit and any interest, dividends, or other income accruing from or generated by such assets, and that may be used to obtain any other funds, goods or services including internet posting services or related services.

Indirect Relationship: A relationship between two parties that affect each other through a third-party source or one or more intermediaries.

Listed Person: Individuals, legal entities and groups listed by the UN Security Council on the UN Consolidated List, or listed by the UAE Cabinet on the Local Terrorist List, as the case may be.

Listing: Identifying the individuals, legal entities and groups subject to sanctions imposed pursuant to relevant UNSC Resolutions ("UNSCRs"), decisions of the Sanctions Committee, or relevant decisions of the UAE Cabinet, as the case may be, and implementing relevant sanctions against such individuals, legal entities and groups, with a statement of the reasons for Listing.

Local Terrorist List: Terrorism lists issued by the UAE Cabinet pursuant to the provisions of Article (63) paragraph (1) of Federal Law No. (7) of 2014 on Combating Terrorism Offences.

Other Measures: Sanction measures other than freezing that must be enforced, and which may be included in Relevant UNSCRs or UAE Cabinet decisions regarding the issuance of Local Terrorist List, such as prohibitions relating to travel, weapons, imports, or provision of fuel supplies and other.

Previous Customer: A customer with whom the relationship was terminated and the LFI maintains relevant records according to record keeping and other requirements.

Relevant UNSCRs: All current and future UNSCRs relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, including but not limited to Resolutions 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.

Sanctions Committee: Any of the UN Security Council Committees established as per its resolutions, including UNSCRs 1267 (1999) and 1989 (2011) relating to ISIL and Al-Qaida, 1988 (2011) relating to the Security and Stability of Afghanistan, and 1718 (2006) relating to the suppression and combating of proliferation of weapons of mass destruction for the DPRK.

Subsidiary: An entity owned by another entity by more than 50% of its capital or under full control of that entity regarding appointment of the Board of Directors.

Targeted Financial Sanctions (TFS): The term Targeted Financial Sanctions means that such sanctions are against certain individuals, entities, groups, or undertakings. The term Targeted Financial Sanctions

includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.

The Executive Office: The Executive Office of the Committee for Goods and Materials Subject to Import and Export Control.

UN Consolidated List: A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their Listing.

Without Delay: Within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

2. SANCTIONS COMPLIANCE PROGRAM

LFIs should take appropriate steps to develop, implement and regularly update an appropriate Sanctions Compliance Program (SCP) in order to fulfil their obligation to comply with the provisions of the Cabinet Decision 74 as well as with the directives of the relevant competent authorities and supervisory authorities in regard to sanctions issued by the UNSC. An appropriate SCP also assists LFIs to manage their exposure to the risks associated with international financial sanctions programs and restrictive measures implemented by other countries.

LFIs should design and update their SCP so that its scope is proportionate to the level of their risk profile, tailored to their nature, scale, and complexity, appropriate for the products and services they offer, the customers, clients, and partner relationships they maintain, and the geographic regions in which they operate. LFIs should ensure the SCP includes the eight (8) essential components: senior management commitment, risk assessment, sanctions risk appetite, internal controls, policies and procedures, training, independent audit and testing of processes and systems, and record keeping.

2.1. Senior Management Commitment

Senior management is defined broadly to include senior leadership, executives, and the board of directors. Senior management's commitment to, and support of, the LFI's SCP is one of the most important factors in determining its success. In order to facilitate effective senior management commitment, an LFI should:

- Ensure that senior management has reviewed and approved the organization's SCP.
- Ensure that senior management has reviewed and approved the methodology used for undertaking the risk assessment and reviewed and approved the LFI's risk assessments at least on an annual basis.
- Clearly designate the personnel responsible for ensuring proper implementation of the SCP, including day-to-day operations, and compliance with statutory obligations. This personnel should have the appropriate competencies and experience, or be appropriately trained, to perform the duties and responsibilities associated with this role, has sufficient seniority, and is delegated sufficient authority and autonomy in order to discharge the LFI's responsibilities. The personnel

may have other responsibilities in the LFI, provided that these responsibilities do not conflict with their role in implementing the SCP. For example, large LFIs may choose to hire a dedicated sanctions compliance officer, while smaller LFIs may choose a specific officer or manager currently working at the LFI to be responsible for the SCP in addition to their other duties.

- Ensure the existence of direct reporting lines between the personnel responsible for the SCP and senior management to facilitate the escalation of financial sanctions issues, including regular and periodic meetings.
- Ensure that the SCP is fully integrated into the organization's daily operations and allocated adequate resources in the form of human capital, expertise, information technology, and other resources as appropriate.
- Recognize compliance failings and implement necessary measures to reduce future incidents, including through addressing root causes and implementing systemic solutions.

2.2. Risk Assessment

LFIs should take appropriate steps to conduct a regular and updated risk assessment to identify, understand, assess, monitor, and manage their risks in line with their business nature and size. While there is no "one-size-fits all" risk assessment, the assessment exercise should generally consist of a holistic review of the LFI from top-to-bottom and assess its touchpoints to the outside world where the LFI may potentially, directly or indirectly, be exposed to sanctioned parties or transactions. In most cases, LFIs should consider performing such risk assessments annually; however, assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. These may include a change to the LFI risk profile, regulatory or law enforcement advisories, or global trends in terrorism financing ("TF") and the financing of proliferation of weapons of mass of mass destruction ("PF").

- In determining potential risks, LFIs should take into account, to the extent relevant, any vulnerabilities relating to:
  - its customers, supply chain, intermediaries, and counterparties;
  - its products and services, including how and where such items fit into other financial or commercial products, services, networks, or systems;
  - the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counterparties;
  - its distribution channels and business partners;
  - the complexity and volume of its transactions;
  - the development of new products and business practices including new delivery mechanisms, channels, and partners; and
  - the use of new or developing technologies for both new and pre-existing products and services.
- LFIs should document risk assessment operations, maintain them up-to-date on an on-going basis, and make them available upon request.
- The results of a risk assessment are integral to informing the SCP's policies, procedures, internal controls, and training in order to effectively mitigate risks.
- LFIs should develop and thoroughly document their risk assessment methodologies to identify, analyze, and address relevant risks. The methodologies should reflect the conduct and root cause of any violations or systemic deficiencies identified.

2.3. Sanctions Risk appetite

LFIs should develop and maintain a comprehensive written sanctions risk appetite approved by the LFI's senior management and embedded through policies, procedures, and screening systems parameterization.

- The sanctions risk appetite should specify which sanctions regimes are applicable to the LFI (for example UNSCR, OFAC, EU, UK etc.).
- LFIs should specify their policy on treating of interests, properties, assets, or entities that are owned or controlled 50% or more by a Listed Person.
- LFIs should specify their approach on mitigating the risk of breaching of unilateral sanctions, especially in the context of sanctions that may have extra-territorial implications or the Listed Persons may or may not have a presence in UAE (for example secondary sanctions by OFAC).
- LFIs should specify their approach on screening of alias names such as one word synonyms, vessel names or paper based instruments.
- LFIs should identify and document any exceptions to sanctions risk appetite or deviations from their policies and procedures; these should be approved by senior management.

For more details and information, please refer to Annex 2 for related Lessons learned from CBUAE Supervision.

2.4. Internal Controls

Internal controls are the mechanisms, rules, and procedures implemented to help ensure the integrity and effectiveness of an LFI's SCP. As required by Cabinet Decision 74, LFIs must have appropriate internal controls in place, including the most recent publication of Targeted Financial Sanctions of the UN Consolidated List and the Local Terrorist List. Accordingly, LFIs must maintain strong and clear internal controls that ensure the effective implementation of their SCP, including policies, procedures, processes, and systems.

- LFIs should document how their processes and systems are configured in order to demonstrate that their configuration is reasonably expected to detect and manage the specific sanctions risks to which the LFI is exposed to and ensure transparency of any system limitations or risk-based decisions that the screening controls are not designed to detect.[4]
- LFIs should establish a mechanism to ensure that, upon learning of a weakness pertaining to its SPC compliance, immediate and effective action is taken to identify compliance gaps and their root causes, including all program-related software, systems, and other technology, and remediate them by implementing systemic solutions to reduce the chances of future failures.

2.5. Policies and Procedures

LFIs should develop and maintain clear and comprehensive written policies and procedures to enable them to manage and mitigate the sanctions risks they have identified, commensurate with the nature and size of their business.

[4] See https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

- LFIs should ensure that policies and procedures are approved by senior management and that they:
  - Enable the LFI to clearly and effectively identify, prevent, escalate, and report suspicious transactions and activities;
  - Are tailored to the organization and capture the organization's day-to-day operations and processes;
  - Are easy to follow and designed to prevent employees from engaging in misconduct;
  - Prohibit employees from, directly or indirectly, informing the customer or any third party that freezing or any Other Measures shall be implemented;
  - Require enhanced due diligence to be conducted on all customers and transactions that are assessed to be high-risk for TF and PF; and
  - Contain sufficient detail of their record keeping obligations.
- LFIs should ensure the effective and consistent implementation of the policies and procedures related to the SCP across their organizations, including branches, Subsidiaries, and other entities in which LFIs hold a majority interest.
- LFIs should clearly communicate the SCP's policies and procedures, including for record keeping, to all relevant employees and external or outsourced service providers.
- LFIs should review and update policies and procedures in a timely manner in response to events or emerging risks and ensure that such updates are communicated to employees on a timely basis.
- LFIs should implement a formal review process at least annually of the policies and procedures at appropriate levels subject to approval where changes are material.
- LFIs should identify and document any exceptions or deviations from the policies and procedures related to the SCP; these should be approved by senior management.

2.6. Training

The maintenance and implementation of an effective SCP requires that all relevant employees and management understand requirements and obligations, policies and procedures, internal control mechanisms, and threats, risks, and vulnerabilities. A robust training program is an integral component of an effective SCP. A training program should:

- Be of a scope and nature proportionate to the LFI's overall risk profile;
- Be specific to the role carried out by the employee, with tailored training for employees engaged in sensitive roles;
- Provide training to all appropriate employees and personnel upon onboarding in a timely manner and at least annually thereafter;
- Hold employees accountable for training through assessments;
- Include measures to take immediate and effective action to provide corrective training or other corrective actions to relevant personnel upon learning of a confirmed negative risk assessment result or audit finding, or other deficiency pertaining to the SPC.

2.7. Independent Audit and Testing of Processes and Systems

Independent audit helps the LFI assess the effectiveness of current processes, including by assessing the sufficiency of the program and by checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify SCP weaknesses and deficiencies. Independent audits should:

- Be undertaken regularly to review and assess the effectiveness of the financial sanctions policies, procedures, systems and controls, and their compliance with the LFI's obligations;
- Be undertaken by the internal audit function, or by a competent independent external auditor, or both, and resourced with skilled and competent staff that understand the SCP of the LFI; and
- Be commensurate to the level and sophistication of the SCP and updated to account for changing risk assessments or sanctions environments.

LFIs should ensure that the audit function is independent of the audited activities and functions, and has sufficient authority, skills, expertise, and resources within the organization. LFIs should immediately address negative audit findings and take the necessary steps to identify and implement compensating controls until the root cause is remediated.

In addition, LFIs should deploy an independent risk-based testing regime to regularly test their processes' and systems' adequacy and expected outcomes, as well as to assess their effectiveness in managing the specific risks articulated in the risk assessment. Regular testing of processes and systems ensures that the screening application generates expected alerts, threshold settings and/or screening rules to forego or suppress undesirable alerts in accordance with the LFI's risk appetite. Regular testing should be supported by metrics, analysis, and reporting, and be reviewed by the personnel responsible for the SPC to determine whether risk acceptance or remediation is appropriate with respect to any relevant findings. Regular testing could be undertaken by the internal audit function, or by a competent external provider, or both.

2.8. Record Keeping

According to the AML-CFT Law and the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as all records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed. LFIs must maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, all depending on the circumstances.

3. SCREENING OPERATIONS

Under Article 21.2 of Cabinet Decision 74, **LFIs must regularly screen their databases and transactions against names on the UN Consolidated List and the Local Terrorist List, and also immediately when notified of any changes to any of such lists,** provided that such screening includes the following:

- Searching their customer databases
- Search for the names of parties to any transactions.
- Search for the names of potential customers.
- Search for the names of beneficial owners.
- Search for names of persons and organizations with which they have a direct or indirect relationship.
- Continuously search their customer database before conducting any transaction, or entering into a serious business relationship with any person, to ensure that their name is not listed on the UN Consolidated List or the Local Terrorist List.

3.1. Sanctions Evasion

Illicit actors targeted by sanctions are likely to utilize a range of tactics to evade the prohibitions, which can be difficult to identify. LFIs should remain vigilant in order to identify attempts to evade, avoid, or circumvent sanctioned activities. Frequent tactics employed for sanctions evasion include renaming, using intermediaries, creating front companies, and using alternative financial networks. LFIs should monitor not only for sanctions violations but also for red flags of potential evasion risks. LFIs also a need to remain vigilant for new methods of evading sanctions. Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") play a critical role, in combination with sanctions screening, to identify and prevent more complicated forms of sanctions evasion.

LFIs should also prohibit activity that aims to evade or circumvent sanctions prohibitions. Accordingly, LFIs must not engage in activities that could be part of a sanctions evasion scheme, including but not limited to:

- Tipping off customers or counterparties;
- Omitting, withholding, altering, misstating, or removing any information about customers or transactions;
- Accepting incomplete (when the customer deliberately does not provide an identifier to obscure being matched with the sanctions lists, such as a date of birth or address) or false information (when the customer provides a false identifier that would not match with the sanctions lists listed details, such as a wrong date of birth);
- Providing false or incomplete information to counterparties or sanctions-imposing authorities; or
- Any other activities that would cause a conflict with or failure to comply with this Guidance.

For more details and information, please refer to the Executive Office's "*Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction*" (circulated by CBUAE Notice No. 2893 dated 02/06/2021).

3.2. Maintenance of UN Consolidated List and Local Terrorist List

LFIs should rely on the official website of the UNSC for the most updated UN Consolidated List:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list

LFIs should rely on the official website of the Executive Office to obtain the most recent publication of the Local Terrorist List issued by the UAE Cabinet:

https://www.uaeiec.gov.ae/en-us/
https://www.uaeiec.gov.ae/ar-ae/

In addition, under Article 21 of Cabinet Decision 74, LFIs must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the Listing and de-Listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.

When LFIs utilize external vendors' lists for their Sanctions List and Local Lists, it is the LFI's responsibility to undertake due diligence on these vendors and ensure that the vendors' lists contain all names listed by the UN Consolidated List and UAE Local Terrorist List.

3.3. Customer Screening

Screening processes should be conducted at various stages of the customer lifecycle to include:

- Periodic name screening: A change to either the customer identifying information or UN Consolidated List /Local Terrorist List should trigger an automatic rescreening.
- Ad hoc name screening: Such screening is triggered by a specific business need or in order to comply with a request by a competent authority, or in the case of feedback from a downstream financial institution.
- Re-screening: A specific scenario in the transaction monitoring system identifies a high-risk jurisdiction in updated customer information.

3.4. Name Screening

In addition to the regular screening utilizing the UN Consolidated List and Local Terrorist List indicated above, LFIs should maintain the following sanctions compliance procedures to prevent and detect sanctions breaches:

1. **Ownership/Control Rule:** Individuals or legal entities that are directly or indirectly owned or controlled mainly or fully by one or more Listed Person are subject to the same prohibitions as the Listed Person, even if such individuals or legal entities are not specifically named by the competent authority on the respective UN Consolidated List or Local Terrorist List.

The criterion to be taken into account when assessing whether an individual or legal entity is mainly **owned** by a Listed Person is the possession of more than 50% of the proprietary rights of an entity or having majority interest in it. If this criterion is satisfied, it is considered that the individual or legal entity is owned by a Listed Person.

The criteria to be taken into account when assessing whether an individual or legal entity or arrangement is mainly **controlled** by a Listed Person, alone or pursuant to an agreement with another shareholder or other third party, include the following:

- Having the right to appoint or remove a majority of the members of the administrative or management body of such a legal person, entity, group or arrangement;
- Having appointed solely as a result of the exercise of one's voting rights a majority of the members of the administrative or management body of a legal person, entity, group or arrangement who have held office during the present and previous financial year;
- Controlling alone, pursuant to an agreement with other shareholders in or members of a legal person, group or entity, a majority of shareholders' or members' voting rights in that legal person, entity, group or arrangement;
- Having the right to exercise a dominant influence over a legal person, group or entity, pursuant to an agreement entered into with that legal person, entity, group or arrangement, or to a provision in its Memorandum or Articles of Association, where the law governing that legal person, entity, group or arrangement permits its being subject to such agreement or provision;
- Having the power to exercise the right to exercise a dominant influence referred to in the previous point, without being the holder of that right;
- Having the right to use all or part of the assets of that legal person, entity, group or arrangement;
- Managing the business of that legal person, entity, group or arrangement on a unified basis, while publishing consolidated accounts; or
- Sharing jointly and severally the financial liabilities of legal person, entity, group or arrangement, or guaranteeing them.

2. **Fuzzy Matching:** An algorithm-based technique to match one data point, where the contents of the information being screened is not identical, but its spelling, pattern or sound is a close match to the contents contained on a list used for screening.

3. **Weak or Low-quality Aliases:** Relatively broad or generic alias may generate a large volume of false hits when such names are run through a computer-based screening system. LFIs should perform their own assessments on whether to screen for weak aliases based on their understanding of their own risk profile.

3.5. Verification of False Positives

Because many names may be common, various potential matches may be found. A potential match is when there is any match between data in the sanctions lists with any information in the LFI's databases. However, it does not necessarily mean that the individual or entity the LFI is dealing with is subject to sanctions. **When identifying the potential match, LFIs should suspend any transaction until they are satisfied it is not a Listed Person.**

LFIs should compare potential matches with the UN Consolidated List and the Local Terrorist List in order to confirm whether they are true matches and to eliminate "false positives." LFIs should compare information that is known about the party in question, such as date of birth and address, with other

information provided in the designation order. Furthermore, LFIs should undertake efforts to obtain additional information and identification documents, which may have previously not been obtained from the customer or a counterparty to ascertain whether the customer is the actual designated person in the case of similar or common names. If the LFI establishes that the match is a false positive, then the LFI does not need to freezing or apply Other Measures related to sanctions. Therefore, the LFI may allow the transaction or relationship to continue its normal course, provided that the transaction or relationship is not suspicious and does not trigger any other concerns. LFIs are required to maintain evidence of the false positive verification process in their records and make them available to the competent authorities immediately upon request.

LFIs may create a "white list" (or a "good customer list") of names of customers that have been flagged as potential matches to the UN Consolidated List and the Local Terrorist List but subsequently cleared through thorough due diligence by the LFI. Those "white lists" may be used to improve the process related to screening by leveraging the results of past due diligences and reducing the number of false positives. While an LFI should not overly rely on such a list and must diligently and continuously screen customers and transactions in case they are implicated in updated UN Consolidated List and Local Terrorist List, the use of such a "white list" may assist the LFI in expediting the dispositioning in case of repeated false positive matches. LFIs should have documented procedures to managing and periodically reviewing and updating those "white lists".

For more details and information, please refer to Annex 2 for related Lessons learned from CBUAE Supervision.

3.6. Payments Screening

LFIs should also screen information regarding counterparties of all incoming and outgoing transfers in order to identify any potential match to Listed Persons. The information to be screened includes:

- The parties involved in a transaction, including the sender and the receiver;
- Third parties and intermediaries;
- Bank Names, Bank Identifier Code ("BIC") and other routing codes;
- Free text fields;
- International Securities Identification Number ("ISINs") or other risk relevant product identifiers (there are multiple fields in the identifier information section for sanctions lists. An ISIN number can be screened as an identifier number similar to a date of birth/passport number, and towns/regions can be screened as jurisdictions operating in);
- Geography, including addresses, countries, cities, towns, regions.

3.7. Confirmed match

Under Articles 15 and 21 of Cabinet Decision 74, when a match is found through the screening process, LFIs must immediately, without delay and without prior notice, freeze all Funds. Without delay, as defined by Article 1 of Cabinet Decision 74, means **within 24 hours** of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

For more details and information, please refer to the Executive Office's *Guidance on Targeted Financial Sanctions for FIs and DNFBPs*.

4. NOTIFICATION TO CBUAE AND EXECUTIVE OFFICE

Under Article 21(5) of Cabinet Decision 74, LFIs must immediately notify the CBUAE in the following cases:

- Identification of funds and actions that have been taken as per requirements of Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Terrorist List (including but not limited to freezing), including attempted transactions.
- Detection of any match with Listed Persons or entities, details of the matched data, and actions that have been taken as per the requirements of Relevant UNSCRs and Local Terrorist Lists, including attempted transactions.
- Identification of a previous customer or an occasional customer listed on the UN Consolidated List or Local Terrorist List.
- Suspicion that a current or previous customer, or a person with whom they have a business relationship, is a Listed Person or has a direct or indirect relationship with a Listed Person.
- No action has been taken due to a false positive and the inability to dismiss a false positive through available or accessible information (i.e. given insufficient information, such as matching identifier information, address, DOB, or nationality). Please see also section 3.5 above.
- Unfreezing of Funds, identifying the information relating to funds that have been unfrozen, including their status, nature, value and measures that were taken in respect thereof, and any other information relevant to such decisions.

Under Article 15(2) of Cabinet Decision, LFIs must also notify the Executive Office of any freezing measures and/or attempted transactions.

According to the Executive Office's *Guidance on Targeted Financial Sanctions for FIs and DNFBPs*, LFIs should notify the CBUAE and the Executive Office within two (2) business days from taking any freezing measure and/or attempted transactions. For the reporting mechanism and form(s), please consult the CBUAE's and the Executive Office's websites as updated from time to time.

Annex 1. Red Flag Indicators for TF and PF

Accurately identifying and assessing the TF and PF risks of a customer or business relationship is critical for appropriately managing these risks. A single indicator on its own may seem insignificant, but when combined with others it could provide reasonable grounds to suspect that the transaction is related to TF or PF activity.

1. Red Flag Indicators for TF

Potentially Suspicious Activity That May Indicate Terrorist Financing Published in the FFIEC BSA/AML Examination Manual[5]

Activity Inconsistent with the Customer's Business:

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers:

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

[5] Available at: https://bsaaml.ffiec.gov/manual/Appendices/07

Other Transactions That Appear Unusual or Suspicious:

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

Terrorist Financing Indicators Published by FINTRAC (Canada's Financial Intelligence Unit)[6]

- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner.
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates individual(s) or entity(ies) may be linked to a terrorist organization or terrorist activities.
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Individual or entity's online presence supports violent extremism or radicalization.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).

[6] Available at: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/fin_mltf-eng

2. Red Flag Indicators for PF

Indicators of Possible Proliferation Financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing[7]

(i) Transaction involves person or entity in foreign country of proliferation concern.
(ii) Transaction involves person or entity in foreign country of diversion concern.
(iii) The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
(iv) Customer activity does not match business profile, or end-user information does not match end-user's business profile.
(v) A freight forwarding firm is listed as the product's final destination.
(vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
(vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
(viii) Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).
(ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
(x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
(xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
(xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
(xiii) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
(xiv) Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
(xv) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
(xvi) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
(xvii) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
(xviii) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
(xix) New customer requests letter of credit transaction awaiting approval of new account.
(xx) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
(xxi) Involvement of items controlled under WMD export control regimes or national control regimes.
(xxii) Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.

[7] Available at: fatf guidance on proliferation financing (fatf-gafi.org)

(xxiii) Use of cash or precious metals (e.g. gold) in transactions for industrial items.
(xxiv) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
(xxv) Involvement of a customer or counterparty, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.
(xxvi) Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.
(xxvii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
(xxviii) Involvement of a university in a country of proliferation concern.
(xxix) Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
(xxx) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.
(xxxi) Use of personal account to purchase industrial items.

3. Red Flag Indicators for Potential Sanctions Circumventions

Some Red Flags or Situations to Identify Potential Sanctions Circumventions Published in the Executive Office's "Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction" [8]

The following are some red flags or situations that could be looked at more closely or monitored by financial institutions and designated non-financial businesses or professions to identify potential sanctions circumventions of your clients, their business, or their transactions.

- Dealings in sectors vulnerable for terrorist financing and/or proliferation of weapons of mass destructions, for example
  - Financial sector
  - Hawalas or other money transfer services providers
  - Oil and gas sector
  - Non-profit organizations
  - International trade
- Dealings, directly or through a client of your client, with high-risk countries for terrorism financing.
- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.
- Dealings with sanctioned goods or under embargo. For example:
  - Weapons
  - Oil or other commodities
  - Luxury goods (for DPRK sanctions)
- Dealings with dual-used goods.
- Dealings with controlled substances.
- Identifying documents that seemed to be forged or counterfeited.

[8] Available at https://www.uaeiec.gov.ae/en-us/un-page#

- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- Use of intermediaries.
- When the flows of funds exceed those of normal business (revenues or turnover).
- The activity developed or financed does not relate to the original or intended purpose of the company o entity. For example:
- For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
- For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.
- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.
- Carrying out of multiple ATM cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or in the border of sanctioned countries.
- Irregularities during the CDD process which could include, but is not limited to:
  - Inaccurate information about the source of funds and/or the relationship with the counterparty.
  - Refusal to honor requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.
  - Suspicion of forged identity documents

Annex 2. Lessons learned from CBUAE Supervision

In 2020 the CBUAE's AML/CFT Supervision Department conducted a thematic review of 30 LFIs' sanctions screening systems. The aim of the review was to assess the LFIs' compliance with these provisions and their sanctions screening systems' effectiveness and efficiency levels.

For more details and information, please refer to the CBUAE's "*Sanctions Screening Testing Thematic Review – Lessons Learned and Expectations".*[9]

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

Annex 3. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding and effective performance by the CBUAE licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE related to targeted financial sanctions, screening and reporting requirements as well as the development of an appropriate sanctions compliance program.
	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, payment service providers, registered hawala providers and other LFIs; and • insurance companies, agencies, and brokers.
Sanctions Compliance Program	Senior Management Commitment	LFI senior management's commitment to, and support of, the Sanctions Compliance Program (SCP) is one of the most important factors in determining its success. In order to facilitate effective senior management commitment, an LFI should, among other things: • Ensure that senior management has reviewed and approved the organization's SCP; • Clearly designate the personnel responsible for ensuring proper implementation of the SCP; and • Ensure that the SCP is fully integrated into the organization's daily operations and allocating adequate resources to it.
	Risk Assessment	LFIs should take appropriate steps to conduct a regular and updated sanctions risk assessment to identify, understand, assess, monitor and manage their risks in line with their business nature and size.
	Sanctions Risk appetite	LFIs should develop and maintain a comprehensive written sanctions risk appetite approved by the LFI's senior management and embedded through policies, procedures, and screening systems parameterization.
	Internal Controls	Internal controls are the mechanisms, rules, and procedures implemented to help ensure the integrity and effectiveness of an LFI's SCP. LFIs must have and maintain strong and clear internal controls to ensure compliance with their statutory sanctions obligations and ensure the effective implementation of their SCP.
	Policies and Procedures	LFIs should develop and maintain clear and comprehensive written policies and procedures that should, among other things: • Be approved by senior management; and • Enable the LFI to clearly and effectively identify, prevent, escalate, and report potentially prohibited transactions and activities. LFIs should ensure the effective and consistent implementation of the policies and procedures related to the SCP across their organizations, including branches, subsidiaries, and other entities in which LFIs hold a majority interest. LFIs should implement a formal review process, at least annually, of the policies and procedures at appropriate levels subject to approval where changes are material.
	Training	A robust training program is an integral component of an effective SCP and should, among other things: • Be of a scope and nature proportionate to the LFI's overall risk profile; • Be specific to the role carried out by the employee, with tailored training for employees engaged in sensitive roles; and • Provide training to all appropriate employees and personnel upon onboarding in a timely manner and at least annually thereafter.
	Independent Audit and Testing of Processes and Systems	Independent audit helps the LFI assess the effectiveness of current processes, including by assessing the sufficiency of the program and by checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify SCP weaknesses and deficiencies. In addition, LFIs should deploy an independent risk-based testing regime to regularly test their processes' and systems' adequacy and expected outcomes, as well as to assess their effectiveness in managing the specific risks articulated in the risk assessment.
	Record keeping	LFIs must maintain, at least for five years, detailed records associated with their ML/FT risk assessment and mitigation measures as well as all records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed; and make them available to authorities on request.

Screening Operations	Sanctions Evasion	LFIs should remain vigilant in order to identify attempts to evade, avoid, or circumvent sanctioned activities. LFIs should monitor not only for sanctions violations but also for red flags of potential evasion risks. LFI's should also prohibit activity that aims to evade or circumvent sanctions prohibitions.
	Maintenance of Sanctions List and Local Lists	LFIs should rely on the official websites of the UNSC and the Executive Office of the Committee for Goods & Materials Subject to Import & Export Control (Executive Office) respectively for the most updated UN Consolidated List and Local Terrorist List. LFIs must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the listing and de-listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.
	Customer Screening	Screening should be conduct at various stages of the customer lifecycle, to include periodic name screening, ad hoc name screening, and re-screening.
	Name Screening	In addition to the regular screening utilizing the lists indicated above, LFIs should maintain additional sanctions compliance procedures relating to name screening to prevent and detect sanctions breaches. These procedures should address the ownership/control rule, fuzzy matching, and weak or low-quality aliases.
	Verification of False Positives	LFIs should compare potential matches with the sanctions lists indicated above in order to confirm whether they are true matches and to eliminate "false positives." If the LFI establishes that the match is a false positive, then the LFI does not need to freezing or apply other measures related to sanctions. The LFI may allow the transaction or relationship to continue its normal course, provided that the transaction or relationship is not suspicious and does not trigger any other concerns. LFIs are required to maintain evidence of the false positive verification process in their records and make them available to the competent authorities immediately upon request.
	Payments Screening	LFIs should also screen information regarding counterparties of all incoming and outgoing transfers in order to identify any potential match to Listed Persons.
	Confirmed Match	When a match is found through the screening process, LFIs must immediately, without delay and without prior notice, freeze all Funds. Without delay, as defined by Cabinet Decision 74, means within 24 hours of the listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.
Notifications	Notifications to the CBUAE and Executive Office	LFIs must immediately notify the CBUAE, as well as the Executive Office, of any freezing measures and/or attempted transactions. LFIs should notify the CBUAE and the Executive Office within two (2) business days from taking any freezing measures and/or attempted transactions. For the reporting mechanism and form(s), please consult the CBUAE's and the Executive Office's websites as updated from time to time.
Annexes	Annex 1	Red flag indicators for TF and PF
	Annex 2	Lessons learned from CBUAE Supervision
	Annex 3	Synopsis of the Guidance