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 SUSPICIOUS TRANSACTION REPORTING

June 7, 2021

Contents

1. Introduction

1.1. Purpose

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

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and 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 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.

1.3. Legal Basis

(AML-CFT Law Articles 9.1, 15, 24, 25, 27; AML-CFT Decision Articles 16-18, 20.2, 21.2, 40-43)

The requirement to submit Suspicious Transaction Reports ("STRs") to the Financial Intelligence Unit ("FIU") is outlined in the (i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations (the "AML-CFT Law"); (ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations (the "AML-CFT Decision"); and (iii) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution.

Under the UAE AML-CFT legal and regulatory framework, all LFIs are obliged to promptly report to the FIU suspicious transactions and any additional information 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. "Crime" is defined in Article 1 of the AML-CFT Law as "money laundering crime and *related predicate offences*, or financing of terrorism or illegal organisations." There is no minimum reporting threshold; all suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. LFIs are also required to put in place and update indicators that can be used to identify possible suspicious transactions.

Although the AML-CFT Law uses the term "STRs" to mean both suspicious transactions and activity, for the purposes of this Guidance document, suspicious activity involving transactions should be reported (in the first instance) to the FIU as STRs; suspicious activity that does not involve transactions, on the other hand, should be reported (in the first instance) to the FIU as Suspicious Activity Reports ("SARs"). Examples of scenarios that warrant a SAR filing include, but are not limited to: the customer is the subject of material adverse media; the customer alerts as a positive sanctions match; the prospective customer acts in a manner that is suspicious upon account opening (e.g., refusing to answer account opening questions; providing falsified or counterfeit documentation; exhibiting reluctance to provide detailed information about a business account, etc.); or the customer exhibits other suspicious behavior (e.g., inquiring about ways to circumvent certain reporting thresholds). STRs, SARs, and other report types (referenced in greater detail in Section 3.2 ("Basic Structure of an STR or SAR")) align with the FIU's current reporting regime and utilization of the goAML system.

Under federal law and regulations, whether the LFIs operate in the mainland UAE or in a Financial or Commercial Free Zone, the designated competent authority for receiving report of suspicious transactions or activity is the FIU. The UAE's minimum statutory obligations that apply to LFIs are covered in the following requirements:

- To put in place indicators to identify suspicious transactions (AML-CFT Law Article 15, AML-CFT Decision Article 16).
- To report suspicious activity to the FIU and cooperate with relevant authorities, including to not disclose the information or data in an STR (AML-CFT Law Articles 9.1, 15, 24, 25, 27, AML-CFT Decision Articles 13.2, 17.1, 18.1, 20.2, 42.1/2).

1.3.1. Consequences for Failure to Disclose Suspicious Activity

Failure to report a suspicious transaction (STR, SAR, or other report types) without delay, whether intentionally or by gross negligence, is a federal crime in the UAE. The AML-CFT Law provides for the following sanctions against any person, including an LFI, or their managers and employees, who fail to perform, whether purposely or through gross negligence, their statutory obligation to report a suspicion of money laundering and related predicate offences or the financing of terrorism or of illegal organisations:

- Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or
- Any of these two sanctions (i.e., imprisonment or fine of no less than AED100,000 and no more than AED1,000,000), according to Article 24 of the AML-CFT Law.

According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a crime.

1.3.2. Protection for Individuals Disclosing Suspicious Activity

LFIs as well as their board members, employees, and authorized representatives, are protected by Article 15 of the AML-CFT Law and Article 17.3 of the AML-CFT Decision from any administrative, civil, or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This is also the case even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. This covers cases when an employee files an STR, SAR, or other report types that its employer did not want to file.

However, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

1.3.3. Meaning of Suspicious Transaction

Within the AML-CFT Law and its AML-CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds for which an LFI has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing - any of the following:

- The proceeds of crime (Money laundering and related predicate offenses, or financing of terrorism or illegal organisations);
- Being related to the crimes of money laundering and related predicate offences, the financing of terrorism or illegal organisations; and
- Being intended to be used in an activity related to such crimes.

The AML-CFT Law and its AML-CFT Decision define a predicate offence as “any act constituting an offense or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.”

It should be noted that the only requirement for a transaction to be considered as suspicious is “reasonable grounds” in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators; financial/transactional and behavioral patterns; Customer Due Diligence (“CDD”) information; or adverse media information, and it is not dependent on

obtaining evidence that a predicate offense has actually occurred or on proving the illicit source of the proceeds involved. LFIs do not need to have knowledge of the underlying criminal activity nor any founded suspicion that the proceeds originate from a criminal activity; **reasonable grounds to suspect any such criminal activity are sufficient.**

LFIs should also note that suspicious transactions need not be completed, in progress, or pending completion. Attempted transactions, transactions that are not executed and past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must be reported in accordance with the relevant requirements.

1.4. Acronyms

Terms	Description
AIF	Additional Information File without Transactions
AIFT	Additional Information File with Transactions
AML / CFT	Anti-Money Laundering / Combatting the Financing of Terrorism and Illegal Organisations
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HRC	High Risk Country Transaction Report
HRCA	High Risk Country Activity Report
KYC	Know Your Customer
QC	Quality Control
Report	Any STR, SAR, AIF, AIFT, RFI, or RFIT based report
RFI	Request for Information without Transactions
RFIT	Request for Information with Transactions
RFR	Reason For Reporting
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report

2. Identification of Suspicious Transactions

2.1. Role of the First Line of Defense

Employees within the first line of defense (e.g., relationship managers, business executives, and back-office operations functions) should understand the AML/CFT risks posed to the business in which they work. First line of defense employees are central to the management of customer and third-party risk and

the timely escalation of potentially suspicious activity. LFIs should not rely solely on transaction monitoring systems to identify unusual and potentially suspicious activity in their customer population. First line of defense employees play a critical role in the detection and prevention of money laundering and the financing of terrorism and illegal organisations. Appropriately trained employees are in fact well-placed to identify suspicious transactions and assess that information once deemed reasonable—collected through interactions with a customer—now appears suspicious. They should therefore be trained regarding potential risk and risk mitigation and reporting within their business area. Employees should understand the regulatory requirements within the scope of their role; red flags associated with their customers, products, services, delivery channels, and geographies; and the appropriate escalation procedure both to their management and to the second line of defense without compromising their responsibility to report suspicious transactions.

2.2. Role of the Second Line of Defense

The second line of defense (e.g., compliance employees) provides policy advice, guidance, assurance, oversight, and challenge to the first line of defense. While employees in Financial Crime Operations Units (possibly in the first line of defense) can investigate suspicious transactions and document the resultant investigation, the ultimate filing of the STR or SAR must be made by the Compliance Officer or the MLRO (in the second line of defense). To this end, the second line of defense is charged with overseeing the investigations programme comprised of both automated and manual monitoring processes. The second line of defense is also charged with monitoring risks facing the LFI, such as noncompliance with UAE laws and regulations, and reporting directly to senior management on the LFI's risk exposure, including through financial crime-related metrics. Specifically, the second line of defense and first line of defense (as applicable) should generate financial crime-related metrics (e.g., STRs or SARs filed, alert backlogs) to provide senior management with an adequate overview of the LFI's compliance program, including the timeliness and quality of the LFI's handling and resolution of transaction monitoring alerts and the STR or SAR filing process. The second line of defense should retain records of all information relating to transaction monitoring and suspicious activity reporting for a period of no less than five (5) years as provided in Article 24 of the AML-CFT Decision.

2.2.1. Role of the Compliance Officer / MLRO

According to Article 21 of the AML-CFT Decision, LFIs are required to appoint a Compliance Officer with the appropriate competencies and experience to perform the necessary tasks to:

- Detect transactions relating to any crime as defined in Article 1 of the AML-CFT Decision.
- Review, scrutinize, and study records; receive data concerning suspicious transactions; and make decisions to either notify the FIU or maintain the transaction with a documented rationale for maintaining the transaction while upholding confidentiality requirements.
- Review the internal rules and procedures relating to combating the crime and their consistency with relevant laws and regulations; assess the extent to which the LFI is committed to the application of these rules and procedures; propose what is needed to update and develop these rules and procedures; prepare and submit semi-annual reports on these points to senior management; and send a copy of that report to the relevant supervisory authority with senior management remarks and decisions.

- Prepare, execute, and document ongoing training and development programs and plans for the LFI's employees on money laundering and the financing of terrorism and financing of illegal organisations, and the means to combat them.
- Collaborate with the supervisory authority and FIU, provide them with all requested data, and allow their authorized employees to view the necessary records and documents that will allow them to perform their duties.

According to CBUAE's Guidelines, the Compliance Officer is the LFI's money laundering reporting officer ("MLRO") charged with reviewing, scrutinizing, and reporting STRs and other reports pertaining to suspicious activity. In this capacity, the Compliance Officer or MLRO is ultimately responsible for the detection of transactions related to money laundering and financing of terrorism and illegal organisations; for reporting suspicions to the FIU; implementing the appropriate actions following an STR, SAR, or other report filing (e.g., ensuring the STR or SAR subject is input into the relevant list for close monitoring or internal watchlists/blacklists; changing the customer risk rating; etc.); and for cooperating with the relevant authorities on AML/CFT matters. The Compliance Officer or MLRO is ultimately responsible to ensure that an appropriate programme exists in the LFI and that the LFI effectively deploys a risk-based approach to detect and report suspicious activity.

The Compliance Officer or MLRO should also act as the primary point of contact with law enforcement agencies for their requests and investigations. The Compliance Officer or MLRO is responsible for liaising with regulators and external bodies on financial crime issues in order to share knowledge, report cases, develop best practices, and where possible, to improve coordination within the financial sector.

2.3. Role of the Third Line of Defense

The independent testing function is responsible for evaluating the design and operational effectiveness of an LFI's compliance program controls, including technical compliance with AML/CFT policies and procedures. This function serves as a "third line of defense" to identify gaps, deficiencies, and weaknesses in operational controls owned or overseen by an LFI's business, operations, and compliance functions. Independent testing should be conducted by an internal audit department, outside auditors, consultants, and/or other qualified, independent third parties. At a minimum, employees responsible for conducting independent testing should not be involved in the function being tested or in other AML/CFT functions that could compromise their independence. Risk-based auditing assists an LFI's Board of Directors and senior management in identifying areas of weakness, prioritizing those areas for remediation, and ensuring the provision of adequate resources, oversight, and training for affected employees.

2.4. Purpose of Transaction Monitoring

The purpose of transaction monitoring is the ongoing, retrospective monitoring of customers' and prospective customers' transactions or activity to identify activity anomalous from normal behavior. This may, on further investigation, generate knowledge or reasonable suspicion of financial crime and thereby require reporting to the appropriate law enforcement and/or regulatory authority as an STR, SAR, or equivalent local report in line with AML/CFT regulatory and/or UAE FIU reporting requirements. LFIs may choose to use a combination of automated transaction monitoring scenarios and exception-based (manual) transaction reports to monitor for potentially suspicious activity. The aim of the alert review process is to identify and respond to potential indicators of money laundering, associated predicate offenses, financing

of terrorism and illegal organisations , financing of proliferation, and any potentially unusual activity that does not align to a customer's or account's profile including by deploying a risk-based approach. An LFI's transaction monitoring systems and manual processes should be reviewed, assessed, and revised periodically—at least annually—and otherwise as appropriate, justified by the required circumstances. Additionally, this review should include both an evaluation of transaction monitoring system thresholds and a fine tuning of the LFI's transaction monitoring system as well as an evaluation of its effectiveness. The individuals responsible for the review should have a proper understanding of the LFI's framework—including the LFI's business and customer base—to generate a meaningful output.

2.5. Internal Organization

In order for an LFI's transaction monitoring and suspicious activity reporting program to be effective, it must be based on the foundation of a sound governance structure. Namely, an LFI's internal organization is important to appropriately identifying unusual or potentially suspicious activity. Internal organization comprises an LFI's policies, procedures, and processes designed to oversee and manage risks and to achieve compliance with UAE AML/CFT laws and regulations. In particular, an LFI's internal organization addresses the core organizational elements of an LFI's compliance program: governance and management oversight; policies and procedures; clear lines of responsibility and reporting; and ongoing training to account for changes in the UAE's legislative and regulatory frameworks.

- Governance and Management Oversight: Governance and management oversight helps to ensure that an LFI's compliance program is appropriately funded, staffed, and equipped with the requisite technology, including to identify and report suspicious activity. An LFI's Board of Directors also ensures that the compliance program has an appropriately prominent status within the organization and is operationally independent. In this capacity, senior management, inclusive of the Compliance Officer, within a compliance program should have the appropriate authority; independence; access to employees and information within the organization; and appropriate resources to conduct their activities—including the identification and reporting of suspicious activity—effectively. The compliance program should have access to the Board of Directors or a designated board committee to raise any issues or risks; report on the status of ongoing compliance; and escalate any other pertinent AML/CFT-related information.
- As part of an LFI's risk management framework, senior management and an LFI's Board of Directors should oversee the design, implementation, and maintenance of a transaction monitoring and suspicious activity reporting program based on an LFI's AML/CFT risks and in accordance with all applicable laws and regulations. Senior management should likewise oversee a vendor selection process (as applicable) if a third-party vendor is used to acquire, install, implement, or test a transaction monitoring program or any aspect of identifying and reporting suspicious activity, among other responsibilities. The Compliance Officer (or MLRO) shall periodically update the Board of Directors (or a committee of the Board) on the overall capability framework (that includes technology and process aspects of suspicious activity identification, investigation and reporting aspects).

- Policies and Procedures: An LFI should have policies and procedures that govern changes to its transaction monitoring program which ensures that changes are defined, managed, controlled, reported, and audited. Namely, LFIs should have governance protocols surrounding the design and implementation of new detection scenarios; periodic assessment and validation of existing detection scenarios; and retiring of detection scenarios. In addition, an LFI should develop a procedure for the investigation and processing of transaction monitoring alerts in order to file an STR, SAR, or other report type promptly and qualitatively. These policies and procedures should cover the key processes for drafting and filing an STR, SAR, or other report type and other regulatory reports. More broadly, policies and procedures work to manage key AML/CFT risks and create processes for adherence across an LFI.
- Clear Lines of Responsibility and Reporting: In relation to suspicious transactions, an LFI should have clear roles, responsibilities, and reporting lines, including reporting and escalations to the Board of Directors and senior management. These roles, responsibilities, and reporting lines should be clearly documented across all three lines of defense. Clear lines of responsibility help with effectively identifying and reporting suspicious activity in a timely manner while ensuring that there is appropriate and effective oversight of employees who engage in activities which may pose greater AML/CFT risk. LFIs should also have a mechanism to inform senior management and the Board of Directors (or a committee of the Board) of compliance initiatives, compliance deficiencies, STRs or SARs (or other reports) filed, and corrective actions taken.
- Ongoing Training: Training should be provided on an ongoing basis to an LFI's employees and should include changes to the UAE's legislative and regulatory frameworks; internal policies or procedures; and understanding of evolving risk issues with respect to an LFI's transaction monitoring and suspicious activity reporting program. Training topics can include, but are not limited to, thematic analysis of STRs or SARs; regulatory requirements and best practices related to STR or SAR reporting; noteworthy STRs or SARs (or other reports) filed during the prior quarter; and controls related to emerging financial crime risks. Training should be customized to include any other internal data that would be beneficial to both the first line and second line of defense.

2.5.1. Considerations for Institutions with Foreign Branches and Subsidiaries

For LFIs operating in an international context, FATF Recommendation 18 recommends that financial groups are required to implement group-wide AML/CFT programs applicable to foreign branches and majority-owned subsidiaries. Recent major enforcement actions taken by supervisors in key jurisdictions have highlighted the need to ensure that systems and controls are aligned across a financial group and that foreign branches and majority-owned subsidiaries align AML/CFT measures with a financial group's home country requirements. As a result, LFIs have implemented global AML/CFT policies that outline a group risk appetite and are managed in each jurisdiction to align to local regulatory or legislative requirements. To support alignment of controls, LFIs operating across jurisdictions may seek to leverage the same control solutions for key processes, such as customer screening or transaction monitoring, though there may be different rules for different jurisdictions. For example, if the LFI operates in an economy which is known to be more cash-based than another, the cash trigger rules in transaction monitoring may vary appropriately. Centralized controls with operational centers of excellence also provide a means of ensuring alignment across the group around systems and controls.

2.6. Transaction Monitoring Methods

The five key components to an effective transaction monitoring and reporting system are: (i) identification of unusual or suspicious activity; (ii) managing alerts with an alert risk scoring model; (iii) STR or SAR decision making; (iv) STR or SAR completion and filing; and (v) monitoring and STR or SAR filing on continuing activity. To effectively identify unusual or potentially suspicious activity, LFIs should first maintain a transaction monitoring program based on an underlying AML/CFT risk-based assessment. The transaction monitoring program should take into account the AML/CFT risks of the LFI's customers, prospective customers, counterparties, businesses, products, services, delivery channels, and geographic markets in addition to helping prioritize high-risk alerts. However, the sophistication of monitoring systems can differ based on an LFI's AML/CFT risks. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or a combination of these. Overall, LFIs must adopt monitoring processes and procedures to monitor customer activity that are commensurate with the size and nature of the line of business and the money laundering and the financing of terrorism and illegal organisations' risks posed by their relevant customer base. The monitoring system and/or manual processes must reasonably demonstrate that transactions that carry the highest risk of money laundering and financing of terrorism and illegal organisations are subject to enhanced scrutiny.

As part of a risk-based approach to AML/CFT, in the case of customers or Business Relationships identified as high-risk, LFIs are expected to investigate and obtain more information about the purpose of transactions, and to enhance ongoing monitoring and review of transactions in order to identify potentially unusual or suspicious activities. In the case of customers or Business Relationships that are identified as low-risk, LFIs may consider monitoring and reviewing transactions at a reduced frequency.

Examples of some of the methods that may be employed for the ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined;
- Transaction-based rules, in which the transactions of a certain type are examined;
- Location-based rules, in which the transactions involving a specific location (either as origin or destination) are examined; and
- Customer-based rules, in which the transactions of particular customers are examined.

2.6.1. Manual Monitoring

An LFI may seek to utilize a manual transaction monitoring system, which typically targets specific categories of transactions (e.g., those involving large amounts of cash, those to or from certain geographies) and includes a manual review of various reports generated by the LFI's systems in order to identify unusual activity. The type and frequency of reviews and resulting reports used should be commensurate with the LFI's AML/CFT risk profile—including the nature, size, and complexity of its operations—and properly cover customers, counterparties, businesses, products, services, delivery channels, and geographic markets. System-generated reports typically use a certain currency threshold to detect unusual activity. An LFI's responsible senior employee should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process and periodically appraise

Senior Management and where required, notify the Board of Directors (as part of periodic updates), on the appropriateness of design of manual monitoring reports. LFIs should be alert to the fact that complex and evolving financial crime risks can undermine the effectiveness of manual monitoring systems, and therefore, manual monitoring systems should also be independently reviewed for reasonable filtering criteria.

2.6.2. Automated Transaction Monitoring

Automated transaction monitoring systems can cover multiple types of transactions and use different rules to identify potentially suspicious activity. In addition, many systems can adapt over time based on historical activity, trends, or internal peer comparison. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps in coverage to address potential financial crime schemes that may not have been addressed. LFIs should also seek to have appropriate case management systems so that such funds or transactions are scrutinized in a timely manner and a determination is made as to whether the funds or transaction are suspicious.

Once established, the LFI should review and test system capabilities and thresholds on a periodic basis, commensurate to its risk profile. This review should focus on specific parameters or filters in order to ensure that intended information is accurately captured, and that the parameter or filter is appropriate for the LFI's particular risk profile, including the applicability of the detection scenarios, underlying rules, threshold values, and assumptions used. An LFI should also aim to review its transaction monitoring program at least annually to account for changes in the LFI's internal procedures; local laws and regulations; and best practices.

Relatedly, the authorization to establish or alter expected activity profiles should be clearly defined through policies and procedures. An LFI's internal controls should ensure limited access to the monitoring systems, and changes should require the approval of the Compliance Officer, MLRO, or senior management. The LFI should implement a robust end-to-end, pre- and post-implementation testing procedure of its transaction monitoring program with documentation detailing current detection scenarios and the underlying assumptions, parameters, and thresholds applied.

Employees appointed by the LFI should also be responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the transaction monitoring program, which may extend to assessing the timely review and decision-making of generated alerts and potential STR or SAR filings. Such employees should be responsible for independently validating an LFI's transaction monitoring system's programming methodology and effectiveness to ensure that the LFI's automated transaction monitoring system is effectively detecting potentially suspicious activity. These appointed employees should also ensure that customer segments, customer types, and transactions/transaction codes are mapped into the transaction monitoring system, and that the transaction monitoring system is integrated with the LFI's core banking and other relevant system. Independent validation should also take place of an LFI's policies with an aim to assess if employees are adhering to these policies. This is especially important to validate the proper use of automated tools and to ensure that the application of information technology instruments or algorithms—often leveraged by LFIs to reduce the number of false positives in their transaction monitoring programs—is not inadvertently suppressing instances of reportable suspicious activity. Where appropriate, the LFI, in lieu of maintaining full time employees to perform aforementioned functions, may hire qualified specialist consultants or external vendors to provide such review services.

2.6.3. Intelligence-led Transaction Monitoring Approach

LFIs have begun to invest in forming and developing their own intelligence units or capabilities. By establishing such units or capabilities, these units seek to maximize the use of data and information available both internally—within the LFI—and externally—across jurisdictions and businesses—in order to tackle money laundering, the financing of terrorism and illegal organisations, and fraud schemes, as well as to consolidate analytical capacity and remove any jurisdictional and business silos. This has led some LFIs to shift from a pure transaction-level monitoring approach towards adopting a "customer-level" or "network" monitoring approach. Under this approach, previous investigations can be applied to inform and refine risk models, which can then be used to customize monitoring for different business lines and customer types. These enhancements are focused on looking beyond single transactions or single customers to identify the wider network in which a customer operates—looking at the customer as an entity—enabling LFIs to manage networks of accounts and report on these networks, that in turn, increases opportunities to disrupt that network. This model moves reporting away from reports of single suspicious transactions towards suspicious entities and networks with a view on how the funds flow between them.

3. Procedures for the Reporting of Suspicious Transactions

All customers and accounts should be subject to monitoring under a risk-based approach in order to identify potentially suspicious transactions, patterns, as well as behavior that is inconsistent with past behavior on the account or with the anticipated activity on the account as determined at onboarding. Alerts on such behavior are risk relevant indicators of potentially suspicious activity. Upon identifying unusual or potentially suspicious activity, an LFI's employees must review and, as appropriate, escalate the activity for further investigation or immediate action.

Although the process for reviewing unusual or potentially suspicious activity for further investigation or immediate action is not outlined in this guidance, LFIs should establish a process to investigate such activity, including developing policies and procedures that document the process for deciding whether to close the alert or to promptly report the transaction as suspicious and should include guidance on capturing detailed descriptions for the manner in which the alerts were either disposed of by reporting or closure of the alerts. For the purposes of this guidance, best practices are discussed once activity is determined to meet one or more of the regulatory definitions of suspicious activity and when an LFI decides to report such activity to the FIU by filing an STR, SAR, or other report type.

3.1. Importance of Filing an STR and SAR

The information generated from an STR, SAR, and other report type is important for identifying and combatting financial crime. First, the quality of STRs, SARs, and other report types is imperative for increasing the FIU's analytical function to identify vulnerabilities and threats to the UAE financial system and develop an overall understanding of money laundering and the financing of terrorism and illegal organisations' risks based on emerging trends and patterns. Relatedly, STRs, SARs, and other report types also assist law enforcement in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system. Law enforcement uses the intelligence generated from STRs, SARs, and other report types to initiate and supplement money laundering or terrorist financing investigations and other criminal

cases. As a result, it is critical that the information provided in all reports of suspicious activity be as accurate, timely, and complete as possible.

3.2. Basic Structure of an STR or SAR

The Compliance Officer or MLRO and other concerned employees responsible for using the goAML system must be aware of the different report types. As such, the LFI should select the correct report type when filing a report through the goAML system. The STR and SAR are the primary (or first instance) reports which must be used to report a new suspicion, whereas Additional Information File without Transactions ("AIF") and Additional Information File with Transactions ("AIFT") report types are supplementary reports which can be used to escalate additional information or transactions that correspond to a previously filed STR or SAR. When filing an AIF or AIFT, the LFI should input the Reference Number that corresponds to the STR or SAR.

- STR: If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or an occasional customer, an LFI suspects transactions are related to money laundering, related predicate offenses, or the financing of terrorism or illegal organisations, then the LFI should submit an STR to the FIU within the timelines established in this guidance.
- SAR: If, during the establishment or course of the customer relationship, an LFI suspects any activity or an attempted transaction (i.e., a non-executed transaction) can be related to money laundering, related predicate offenses, or the financing of terrorism or illegal organisations, then the LFI should submit a SAR to the FIU within the timelines established in this guidance.
- Additional Information File ("AIF") without Transactions: Should the FIU require any further details while reviewing an STR or SAR, then the LFI that originally submitted the report may be solicited for further information by receiving an AIF request from the FIU through the Message Board. Should such a situation arise, the LFI is required to submit an AIF based report through the goAML platform. Please note that an AIF is a supplemental report that does not contain transactional details.
- Additional Information File with Transactions ("AIFT"): Should the FIU require any further details including transactions while processing an STR or SAR, then the LFI that originally submitted the said report may be solicited for further information including transactions by receiving an AIFT request from the FIU through the Message Board. Should such a situation arise, then the LFI is required to submit an AIFT report through the goAML. Please note that an AIFT is a supplemental report that contains transactional details.
- Request for Information ("RFI") without Transactions: Should the FIU require further information from multiple LFIs rather than just the entity responsible for submitting the STR or SAR, then an RFI request will be sent out to the concerned LFIs through the goAML Message Board. Should such a situation arise, then the LFI is required to submit an RFI report through the goAML portal.
- Request for Information with Transactions ("RFIT"): The 'RFI with Transaction(s)' report is similar to the structure of an RFI request, with the exception that this report type supports the use of transactions.
- High Risk Country Transaction Report ("HRC"): If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or a potential customer, an LFI identifies transactions related to high-risk countries as defined by the National

Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee[2], then the LFI should submit an HRC to the FIU. Such reported transaction(s) may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.

- High Risk Country Activity Report ("HRCA"): If, during the establishment or course of the customer relationship, or when conducting an activity on behalf of a customer or a potential customer, a reporting entity identifies activities related to high-risk countries as defined by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee[3], then the entity should submit an HRC to the FIU. Such reported activity(ies) may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the activity within the set period.

When all applicable information is collected, analyzed, and documented and the LFI decides that an STR or SAR is required, the information should be described in the narrative within an investigative narrative report template in a concise and chronological format. The LFI should divide the narrative into three sections: an introduction, a body, and a conclusion. The investigative narrative report template is considered as an addition to the goAML report (due to the potential text limitation within the "goAML description of the report" field).

- **Introduction**

The introductory paragraph should provide:

- A brief statement addressing the purpose of the report with a general description of the known or alleged violation.
- The name(s) of the subject against whom the report is filed.
- Any linked/ previous STRs, SARs, or other reports, including the date of any STR(s) / SAR(s) filed (or other reports) previously on the suspect or related suspects and the reason why the previous STR(s) / SAR(s) (or other report) was filed.

Additional Guidance:

- Whether the activity is associated with any sanctioned countries or contained on government lists for individuals or organisations.
- A summary of the "red flags" and suspicious patterns of activity that initiated the report. (This information should be provided either in the introduction or conclusion of the narrative).

- **Body**

The next paragraph or paragraphs of the narrative can provide all pertinent information documenting why the STR, SAR, or other report was filed and might include:

- Details of parties facilitating the suspicious activity or transactions. If the subject is an entity, details of the subject can include the entity's trade license number, date established, line of business, licensing authority, and ownership structure.

[2] https://www.namlcftc.gov.ae/en/high-risk-countries.php
[3] Idem note

- Involved suspected transactions (usually identified in chronological order by date and amount) [To be included only for an STR and supplementary reports involving transactions].
- The review period for the suspicious activity or transactions.
- The source of funds, destination of funds, and total of suspected amounts. This can include the transactor and beneficiary information, providing as much detail as possible, including the name and location of any involved domestic and/or international financial institution(s); names, addresses, account numbers, and any other available identifiers of originator and beneficiary transactor(s); and/or third parties or business entities on whose behalf the conductor was acting; the date(s) of the transaction(s); and amount(s).
- Explain in detail the reason for the suspicion, and why the activity or transaction is determined to be illegal or suspicious.
- Description of the method of operation (i.e., modus operandi).

Additional Guidance:

- A breakdown of larger volumes of financial activity into categories of credits and debits, and by date and amount. [To be included only for an STR and supplementary reports involving transactions].
- An explanation of any observed relationships among the transactors (e.g., shared accounts, addresses, employment, known or suspected business relationships and/or frequency of transactions occurring amongst them; appearing together at the LFI and/or counter). [To be included only for an STR and supplementary reports involving transactions].
- Specific details on cash transactions that identify the branch(es) where the transaction(s) occurred, the type of transaction(s), and how the transaction(s) occurred (e.g., night deposit, on-line banking, ATM, etc.). [To be included only for an STR and supplementary reports involving transactions].
- Any factual observations or incriminating statements made by the suspect.

- **Conclusion**

The final paragraph will be covered under “Action Taken by Reporting Entity” field. The final paragraph of the narrative can summarize the report and might also include:

- Any planned/initiated mitigating steps, including information about any follow-up actions conducted by the LFI (e.g., intent to close or closure of accounts, ongoing monitoring of activity, etc.).

Additional Guidance:

- Names and telephone numbers of other contacts at the LFI if different from the point of contact indicated in the report.
- A general description of any additional information related to the LFI that may be made available to law enforcement by the LFI.
- Names of any law enforcement or department/unit investigating the case who are not already identified in another section of the report.

3.3. Best Practices for Drafting an STR or SAR

In general, a narrative should identify the five core components – who? what? when? where? and why? – of the suspicious activity being reported to the FIU. The method of operation/modus operandi (or how?) is also important and should be included in the report narrative. An LFI should ensure that the following five questions are answered prior to submitting an STR, SAR, or other report in the FIU's goAML system.

Who is conducting the suspicious activity or transaction?

- Describe the **subject of the STR, SAR, or other report**, otherwise known as the suspect(s), including the conductor, beneficiary, and accountholders involved in the transaction or activity.
- Provide **identifying information** on the parties involved in the transaction, such as the suspect's occupation and position or title within the business.
- List **beneficial owners, directors, officers, and those with signing authority**, if possible. If the transaction or activity involves an entity, include information on the ownership, control, and structure of the business.
- Provide **details about each individual or entity's role** in each of the financial transactions described. It is important to understand who is sending and receiving the funds. [To be included only for an STR and supplementary reports involving transactions].
- If more than one individual or entity is involved in the suspicious activity, **explain the relationships among the individuals or entities (if known).**

Even though information may not always be available, information should be included to the extent possible. For instance, addresses for suspects are important; filing LFIs should note not only the suspect's primary street addresses, but also, other known addresses. Any identification numbers associated with the suspect(s) such as passport and driver's license numbers are also important to document.

What instruments or mechanisms are being used to facilitate the suspicious activity or transaction(s)?

- Review the **instruments or mechanisms used in the suspicious activity** (e.g., wire transfers, foreign currency, Wages Protection System (WPS), letters of credit and other trade instruments, correspondent accounts, money orders, credit/debit cards, etc.).
- Understand the **number of different methods employed for initiating the negotiation of funds**, such as the Internet, phone access, mail, night deposit box, remote dial-up, couriers, or others.
- Describe the **source of the funds (as originator) or use of the funds (as beneficiary).** In documenting the movement of funds, **identify all account numbers at the LFI affected by the suspicious activity or transaction** and when possible, provide any account numbers held at other LFIs and the names/locations of the other LFIs involved in the reported activity.

When did the suspicious activity or transaction take place?

- If the activity takes place over a period of time, **provide the date** when the suspicious activity or transaction was first observed and describe the duration of the activity.
- To better understand the history and nature of the activity, and the flow of funds, LFIs should provide **information on each individual transaction** in a chronological order (e.g., individual

dates and transaction amounts, rather than only the aggregated amount). [To be included only for an STR and supplementary reports involving transactions].

- Provide information on when **the transaction was completed or attempted**. If the transaction was not completed, the LFI should indicate this in the narrative. [To be included only for an STR and supplementary reports involving transactions].

Where did the suspicious activity or transaction take place?

- Explain if **multiple offices of a single LFI** were involved in the suspicious activity or transaction being reported. Provide the addresses of those locations.
- Specify if the **suspected activity or transaction(s) involves a foreign jurisdiction**. In this case, list the foreign jurisdiction, LFI, address, and any account numbers involved in, or affiliated with the suspected activity or transaction(s).
- This information should include any location involved in the **full transaction chain**, including ultimate originators and beneficiaries to the extent this can be ascertained. [To be included only for an STR and supplementary reports involving transactions].

Why does the LFI think the activity or transaction is suspicious?

- Describe the **industry or business** and why **the activity or transaction is unusual** for the customer. Consider the **types of products and services involved** in the activity and the **expected activities** of similar customers.
- Assess **why the activity created a red flag** for the LFI or triggered an alert within the system.

These answers will vary based on the LFI type (for example, a depository institution versus an insurance company) and an LFI should also consider such factors as:

- The types of products and services the LFI offers;
- The types of accounts the customer has with the LFI;
- The normally expected business activity of the customer (if they are a customer of the LFI), and why this is not normal or expected activity;
- The purpose of the payment or transaction, to the extent known, reported, alleged, or questioned; and
- If the activity resulted from an automated alert, the scenario or rule that generated the alert.

How did the suspicious activity or transaction occur?

- Describe how the **transaction or pattern of transactions was committed** (i.e., the “modus operandi” or the method of operation). [To be included only for an STR and supplementary reports involving transactions].
- For example, if there appear to be multiple cheques deposited matched with outgoing wire transfers from the accounts, the narrative should include information about both the cheques and outbound transfers (including dates, destinations, amounts, accounts, frequency, and beneficiaries of the funds transfers).

3.3.1. Defensive STR or SAR Filings[4]

Defensive filing is the practice of filing STRs or SARs on transactions or activity(ies) that LFIs do not deem truly suspicious in order to reduce the risk of regulatory penalties for non-filing of STRs or SARs.[5] Although there may be some aspect of the transaction or activity creating potential suspicion, defensive filings do not report on activity that the LFI truly considers suspicious. As such, defensive filings are generally discouraged given that such filings diminish the value of STRs and SARs, including by leading to an increase in non-valuable filings. An STR, SAR, and other report types should be of the best possible quality, including in that it should have a clearly written narrative with sufficient detail that comprehensively articulates the factors involving the reported suspicious transaction or activity. As a result, the CBUAE considers defensive STR or SARs as indicative of an inefficient transaction monitoring system and an LFI's weak system of internal controls. An LFI may be asked to correct such deficiencies as part of broader supervisory measures provided by applicable law, including administrative sanctions, temporary limitation to business activities, etc. If, for any reason, an LFI needs additional data to assess whether unusual activity is truly suspicious, the LFI should review other mechanisms—such as expanding the time period for reviewing alerted transactions (e.g., from 30 days to 90 days) or reviewing threshold-based reports—to make the determination that an STR or SAR is required.

3.4. How to Submit an STR and Other Report Types

LFIs are required to submit suspicious transaction and activity reports directly to the FIU using the "goAML" portal, and registration in the system is mandatory for all entities under CBUAE's supervision. According to the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions, the FIU has launched the goAML system for the purposes of facilitating the filing of STRs, SARs, and other report types by all LFIs. LFIs should register themselves on the goAML system by following the "GoAML Registration Guide" and maintaining their registration in an "active" status. An entity's Compliance Officer or MLRO can register as the user of the system. GoAML provides a secure link from each LFI to the FIU through their respective supervisory authorities. The system also has an .xml schema for filing batches of STRs. All newly licensed LFIs should register themselves immediately after obtaining their financial services license. Failure to register within the goAML system may result in a breach of the LFI's AML/CFT obligations and will be dealt with in accordance with the prevailing legal provisions related to non-compliance.

According to the "goAML XML Submission Guide," the goAML system reflects multiple mandatory fields, business rules, and various binding scenarios. Combined, the system only accepts reports that pass through the minimum requirements set by the FIU. Mandatory fields for submitting a report in the goAML system are noted below:

[4] The UAE FIU has noted instances where SAR or STRs are reported due to the LFI not receiving supporting documents that would justify the transaction or activity. However, upon the FIU raising a request to the same LFI in the form of an AIF, supporting documents were subsequently provided for the same subjects and report. This documentation in some instances removed the suspicion of the transaction and in others, helped explain the transaction or action. Submitting reports to the FIU without first conducting a thorough investigation and looking at all available evidence creates a situation where non-suspicious transactions may be reported to the FIU. LFIs are reminded that internal investigations into the suspicious transaction or activity should be conducted to the fullest extent possible prior to raising an STR or SAR and that related documentation, when available or easily retrievable, should be included with the STR or SAR.

[5] Egmont Group, Enterprise-wide STR Sharing: Issues and Approaches, Pg. 17

1. **Select the Report Type [4.2.1 GoAML XML Submission Guide]:** A Compliance Officer or MLRO should select a report type and populate all available details in the 'Report Cover' as depicted below:

• Reporting Entity ID – Entity name as per the registration (auto-generated) • Internal STR/SAR # – Internal STR/SAR number • Submission Date* – Date of escalating the Report to the FIU (auto-generated) • Description/Summary of the Report* – Brief overview for the suspicion/reason for submitting this report to the FIU. This field is only mandatory for STR and SAR report types • Reporting Entity Branch – Branch where the main subject(s) of the report were identified	• Report Type* – Report type relevant to the suspicion/reason for submission to the FIU • FIU Reference – Only applicable in the case of AIF/RFI/ AIFT/RFIT type reports. Provide the corresponding case number as specified in the Message Board communication sent by the FIU • Action Taken by Reporting Entity* – The action(s) taken by the reporting entity post-identifying the reason for suspicion/submission

2. **MLRO Details [4.2.2 GoAML XML Registration Guide]**: This section of the report includes details on the Compliance Officer, MLRO, or individual filing the report, which is automatically populated using the details provided during the registration phase.[6]
3. **Location of the Incident [4.2.3 GoAML XML Registration Guide]**: The location of the incident requires the location where the suspicious incident/transaction originated from. This is mandatory for STR and SAR report types.
4. **Reason for Reporting [4.2.4 GoAML XML Registration Guide]**: The LFI is expected to select the most appropriate reason for reporting available from the menu selection provided. If necessary, more than one reason may also be provided. It is imperative that the *correct* Reason for Reporting ("RFR") is chosen for STRs or SARs submitted in the goAML system.[7]
5. **Transactions [4.2.5 GoAML XML Registration Guide]**: If the reported activity involves transaction(s), the LFI should populate the following transaction details:

• Transaction Ref. Number* – Kindly use the auto-generate button to generate a unique identification number if the LFI is not a Bank/Exchange House	• Transaction Executed by (Staff Name) – Name of the staff member who executed the transaction

[6] The UAE FIU has noted that there have been instances of reports being received whereby upon review, the LFI's MLRO and related team members' contact details were not updated in the goAML system, which included email addresses and phone numbers. Keeping contact information updated helps with the two-way communication between LFIs and the FIU while helping to shorten the turnaround time of report analysis. It also enhances the ability of the FIU to analyze and subsequently process reports in a timely manner. The contact information should be kept updated at all times.

[7] The UAE FIU has noted that in some cases LFIs file reports while choosing RFRs that, upon closer examination, are not linked to the actual suspicions of the report. As an example, reports have been received with RFRs related to the financing of terrorism and illegal organisations with no evidence of any activity connected to the financing of terrorism and illegal organisations. Selecting incorrect RFRs hinders the FIU's analysis, and the LFI should expect multiple requests by the FIU for further clarification in these cases. LFIs should be prudent and diligent when choosing RFRs and submitting reports to the UAE FIU. RFRs should be chosen correctly and in relation to the actual suspicions of the STR or SAR being submitted.

• Reporting Entity Internal Reference Number* – Reporting entity's internal transaction reference number • Type of Transaction* – The mode used to conduct the transaction being reported • Late Deposit – Does this transaction account as a late deposit? (Yes or No) • Total Suspected Amount* (AED) – Suspected amount in AED • Date* – Date when transaction was initiated • Indemnified for Repatriation* – If the reporting entity has received an indemnity for repatriation	• Authorizer – Name of the staff member responsible for authorizing the transaction • Branch executing the transaction* – Branch where the transaction was executed • Date of receipt for recall request* (that field will only show if 'Yes' was selected for Indemnified for Repatriation) – The date when the reporting entity received the fund recall request • Purpose of the Transaction* – Purpose for executing the transaction • Transactions Comments – Comments (if any)

6. **Transaction Type, From Type / To Type, My Client / Not My Client, Foreign Currency, Conductor, [4.2.5.1-4.2.5.5 GoAML XML Registration Guide]:** Additional transaction details should be added according to the transaction type; transaction type (to/from) (i.e., my client, not my client); and foreign currency type (if applicable); and the amount. These fields should be populated by the LFI according to the GoAML XML Registration Guide's instructions. Please refer to Party Type: Person (below) to populate information on the conductor of the transaction for 4.2.5.6.
7. **Phone, Address, Identification, Email, and Employer Address and Employer Phone [4.2.5.7-4.2.5.11 GoAML XML Registration Guide]**: These fields should be populated by the LFI according to the GoAML XML Registration Guide's instructions.
8. **Party Type [4.2.5.12 GoAML XML Registration Guide]**: The 'Party Type' refers to the initiating source (source of funds) and beneficiary/destination party in relation to the report being filed. The initiating source and beneficiary/destination party can be either a Person, Account, or Entity.

    - **Party Type: Person [4.2.5.6, 4.2.5.13 GoAML XML Registration Guide]**: Where the subject initiating or receiving the transaction is a person, clicking the 'Person' radio button will generate the following form and fields.

• Title – e.g., Mr./Mrs./Dr. • Prefix – Prefix Name e.g., Von, Jr. • First Name* – First name of the person • Middle Name – Middle name of the person • Last Name* – Last name of the person • Gender – Male / Female • Birth Date – Date of birth of the subject person • Birthplace – Location where the person was born • Mother's Name – Name of the person's mother (if available)	• Occupation – Known occupation of the subject • Employer Name – Name of the person's current employer • PEP (Y/ N) – Specify if the person is a politically exposed person. Input "Y" or "N" accordingly • Source of funds – Primary source of funds used for the reported transaction • Passport* – Select if the passport details are available (Y/N)

• Alias – A known alias for the person (if applicable) • Emirates ID – Emirates ID number; input the number without using any spaces/hyphens • Nationality 1 – First nationality of the person • Nationality 2 – Second nationality of the person • Nationality 3 – Third nationality of the person • ID Number – ID number; input the number without using any spaces/hyphens • Tax Number – Tax number for outside UAE without hyphens/spaces (e.g., FATCA number for US citizens) • Residence – Country of residence	• Passport Number* – Input the passport number without any spaces/hyphens only in the absence of an Emirates ID • Passport Country* – Country of the passport provided • Deceased – Is the person deceased? (Y/N) • Date of Death – Date when the person died (applicable only if "Y" was provided in the 'Deceased' field)

- **Party Type: Account [4.2.5.14 GoAML XML Registration Guide]:** If the transaction was initiated or received through an Account, clicking the 'Account' radio button will generate the following form and fields:

• Account Number* – Account number without any spaces/ hyphens • Status Code (is mandatory for My Client) – Account status when transaction was initiated • Institution Name – Name of the institution where the account was created • UBO* – Who is the beneficial owner of the account? • Non-Banking Institution – Is the mentioned account held in a bank or otherwise (Y/N) • Client Number – Client Number as per reporting entity's records • Account Type – Drop-down menu for type of account • Currency Code – Currency of the account • IBAN – IBAN as per standard format (no spaces/hyphens) • Opened* – Date of account opening	• Closed – Date of account closure • Balance* (Y/N) – Input "Y" or "N" on whether there is a credit / debit in the account • Balance (if the 'Yes' radio button is selected (above)) – The current balance of the account in AED • Date of balance – Date when the balance was recorded

- Please note that LFIs should also add a 'Signatory(ies)' form for reports involving accounts that are classified as 'My Client.' When the accountholder is a person, the LFI is required to enter all involved signatories. If the accountholder is an entity, the LFI is required to populate the entity details. For instances where an account has multiple signatories, all of the signatory details need to be captured in the goAML system.

- **Party Type: Entity [4.2.5.15 GoAML XML Registration Guide]:** If the transaction was initiated through an Entity, clicking the 'Entity radio button will generate the following form and fields.

• Name* – Legal name as per documentation • Commercial Name – Commercial name as per documentation • Business Activity – Business activity of entity (drop-down) • Licensing Authority – Regulatory authority responsible for licensing the entity • Trade License Number Authority • Place of incorporation – Specify the city (Emirate in case of a UAE entity) • Establishment Date – Date when entity was established • Incorporation Country – Country where the entity was incorporated (drop-down) • Email – Registered email for the entity (if any) • Website – Website for the entity (if any) • Tax Number – Tax number for outside UAE without hyphens/spaces (e.g., FATCA number for US citizens)	• Comments – Comments (if any) • PEP (Y/ N) – Specify if the person is a politically exposed person. Input "Y" or "N" accordingly • Latest date of trade license issuance/renewal – Date of trade license issuance/renewal • Latest date of trade license issuance/renewal – Date of trade license issuance/renewal • **Phones, Addresses, and Controlling Persons/Beneficial Owners can also be added. Addresses and Controlling Persons/Beneficial Owners section are mandatory only when the entity is classified as 'My Client.'

9. **Involved Parties [4.2.5.16 GoAML XML Registration Guide]:** If there are multiple parties involved in the reported activity, the 'Involved Parties' form should be populated with the following fields.

• Role* – Nature of association with the transaction • Funds Code* – The type of funds • Country* – Country of the involved party • Significance – Rate the significance of the concerned subject from 0 - 10 (0 being the lowest and 10 being the highest score)	• Funds comment – Comments on use of funds (if any) • Comments – Comments (if any) • **Foreign Currency can also be added

10. **Good and Services [4.2.5.17 GoAML XML Registration Guide]**: This section corresponds to transactions involving the exchange of goods and services.

• Item Type* – The type of item (e.g., Vehicle) • Description – Description of the item (e.g., Luxury Car) • Manufacturer – Item maker (e.g., if the item is a car - BMW) • Presently Registered To – Name of current owner • Previously Registered To – Name of previous owner • Status Code – Stats code (e.g., Bought, Hired) • Estimated Value – Estimated value of the item • Currency Code – Used to report service conducted in foreign currency •	• Disposed Value - Effective value for property transfer (value must be in AED) • Size UOM – Unit of measurement (e.g. square meters) • Size – Size of the property • Registration Number – Official registration number (e.g., Car VIN Number) • Registration Date – Official registration date (in MM/DD/ YYYY format) • Identification Number – Any number that can identify the item (e.g., Car Plate Number) • Comments – If applicable • **Addresses can be added

11. **Activity [4.2.6 GoAML XML Registration Guide]:** If the report does not contain any transaction(s), then the activity details may be captured in the report. The activity details should include the significance of a concerned subject (scale of 0-10), the reason for reporting the party, and any comments. The 'Activity' tab will be shown only in the case the reporting entity is submitting an "SAR", "RFI without transaction(s)" or an "AIF without transaction(s)" based report file.

Upon completion of all the mandatory fields (noted above) and submission of the report in the goAML system, the report will be provided to the FIU. It is mandatory for the LFI's filer to attach **supplemental documents** to accompany the submission—including but not limited to—Know Your Customer ("KYC") documentation, copies of identification documentation, account opening forms, transaction receipts, financial statements, and other documents relevant to the investigation. In the instance that the LFI conducted due diligence or internal investigations, the corresponding documents must also be attached. This will assist the FIU in reviewing the report with all the appropriate documentation to support its review and analysis.

3.5. Amendments to Submitted Reports

Once a report is submitted and accepted in the system, neither the Compliance Officer, MLRO, nor FIU employees can apply any changes and amendments to the report for missing or incorrect information. However, LFIs may be requested to file a corresponding AIF, AIFT, RFI, or RFIT, and mention in the "Description of the Report" field the reason of filing. LFIs should ensure that the filer uses the correct web reference number of the initial report. In order to avoid such incident(s) and in order to safeguard the system data integrity, LFIs should adopt a maker and checker process/concept to verify the quality and accuracy of uploaded information.

4. Timing of Alert Reviews and STR or SAR Filings

4.1. Alert Review, Case Investigation, and STR or SAR Decision Making

An efficient alert management and dispositioning process is essential to safeguarding the financial integrity of LFIs, assisting law enforcement in the identification and investigation of criminal activity, and satisfying regulatory expectations concerning timely suspicious activity reporting. The alert management and dispositioning process should be adequately staffed and free of bottlenecks and should include a process for the expedited filing of urgent reports in appropriate cases. For purposes of this guidance, "alerts" shall be understood to include automated transaction monitoring alerts, employee referrals, and law enforcement requests. The LFI should apply a risk-based approach to the alert review process by prioritizing alerts based on their risk category. For instance, alerts generated on suspicious transactions of higher-risk customers should be risk-scored higher and prioritized for review.

Alert Review: An LFI's employees should review an alert and determine whether further investigation is warranted. The underlying basis for the determination should be documented in accordance with an LFI's investigations procedures. An LFI may choose to have alert review decisions subject to Quality Control ("QC") review, prior to final dispositioning.

Where the facts available at the alert review stage are or may be sufficient to warrant an STR or SAR filing without further investigation, or where the transaction may otherwise require immediate attention (per criteria set forth below in 4.4 Activity Requiring Immediate Attention), employees should immediately escalate the alerted activity to the designated STR or SAR decision authority for expedited review.

Case Investigation: For any alerted activity determined to require further investigation, employees should conduct and complete (at least preliminarily) an investigation of the alerted activity, document the results of any research or analysis performed, and make a recommendation as to whether an STR or SAR should be filed.

Where a case investigator becomes aware of activity that requires immediate attention (per criteria set forth below in 4.4 Activity Requiring Immediate Attention), employees should immediately escalate the activity to the designated STR or SAR decision authority for expedited review.

If, in the case investigator's judgment, the facts available at the filing recommendation deadline meet one or more of the UAE regulatory definitions of suspicious activity, the case investigator should submit a recommendation to file an STR or SAR, even if certain aspects of the activity remain unexplained. Unanswered requests for information (RFIs) made in the course of a case investigation should not delay the timely submission of recommendations with respect to an STR or SAR filing. LFIs should define the reasonable RFI timeframe to allow the customer to respond to quires raised during a case investigation as part of the RFI process. This RFI timeframe should be within 20 days from the date of alert generation.

STR or SAR Decision Making: In the absence of escalation for expedited review, the Compliance Officer or MLRO should review a case investigation recommendation and make a determination as to whether the activity is suspicious within 20 days of the date of alert generation.

In the event of escalation for expedited review, the Compliance Officer or MLRO should review the activity and make a determination as to whether it is suspicious within 24 hours of the date of escalation. Where appropriate, the Compliance Officer or MLRO also should escalate the activity for potential exit and account closure.

4.2. STR or SAR Filing

In the absence of escalation for expedited review, the Compliance Officer or MLRO should file an STR or SAR to the FIU within 15 days of the date of determination that a transaction meets the definition of suspicious activity. In the event of escalation for expedited review, the Compliance Officer or MLRO should file an STR or SAR to the FIU within 24 hours of the determination. All prospective STRs or SARs should be reviewed for accuracy and completeness prior to filing, in accordance with applicable procedures.

4.3. Monitoring and Reporting of Continuing Suspicious Activity

Employees should review any new activity involving a previous STR or SAR subject within 90 days of the last reported transaction. Where such a review uncovers continuing suspicious activity, employees should file an STR or SAR no later than 105 days from the date of the previous STR filing. There may be situations that require filing an STR or SAR sooner than 105 days after the initial STR or SAR. A 'post-STR or SAR' review can be achieved either manually or via an LFIs' automated and ongoing transaction monitoring systems/scenarios.

4.4. Activity Requiring Immediate Attention

Situations requiring immediate attention include reportable violations that are ongoing (e.g., part of an ongoing money laundering scheme as indicated by an appropriate law enforcement authority) and transactions that the LFI suspects are related to the financing of terrorism and illegal organisations.

4.5. Exceptions for Complex Investigations

There may be instances when the LFI encounters potentially unusual or suspicious activity that is of a "complex" nature. The following is a non-exhaustive list of factors that should be considered to determine whether investigated activity qualifies as a complex investigation: employee-related investigations; significant investigations involving multiple customers, multiple jurisdictions, multiple accounts, multiple transactions, and/or multiple subpoena requests; and legal referred investigations.

If the LFI designates an investigation as "complex," the LFI should submit an initial STR or SAR filing within 15 days of determination that the activity is suspicious, and the STR or SAR filing should be annotated as a "complex investigation" to the FIU. Following the initial STR or SAR filing, the LFI has an additional 30 days to obtain all necessary information related to the complex investigation and submit a follow-up STR or SAR to the FIU.

4.6. Summary of Review, Investigation, and Reporting Timelines

The following table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the absence of escalation for expedited review. Please note – the following table captures the *maximum* timeline by which LFIs should identify and report suspicious activity and transactions. LFIs are ultimately responsible under UAE's AML-CFT Law to report suspicious activity *without delay* and should seek to file STRs and SARs ahead of the below timelines.

Action	Maximum Timeline in Calendar Days
Dispositioning of alert; recommendation on whether to file an STR or SAR; and decision on whether to file an STR or SAR	Within 20 days of alert generation
Filing of first STR or SAR	15 days from decision to file *(35 days from alert generation)*
Filing of a follow-up STR or SAR for a "complex investigation"	30 days from first STR or SAR filing (*65 days from alert generation*)
Filing of STR or SAR on continuing activity	105 days from previous STR or SAR

4.7. Escalation for Expedited Review

In certain cases, an alert or case may need to be dispositioned and an STR or SAR filed more rapidly than usual processes allow. In such cases, the alert will be dispositioned and the STR or SAR filed according to the expedited review timeline as laid out below.

Circumstances where expedited review is expected include:

- The activity requires immediate attention (as defined above); and
- The facts available at the alert review stage are or may be sufficient to warrant an STR or SAR filing without further investigation.

The following table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the event of escalation for expedited review.

Action	Maximum Timeline in Calendar Days
Decision on whether to file an STR or SAR and filing of first STR or SAR	24 hours from decision to file
Filing of STR or SAR on continuing activity	105 days from previous STR or SAR

5. Confidentiality and Prohibition against "Tipping Off"

According to Article 18 of the AML-CFT Decision, when reporting suspicious activity or transactions to the FIU, LFIs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure that the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT framework, and in keeping with the nature and size of their businesses, LFIs and their foreign branches or group affiliates where applicable, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs, SARs, and other report types. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organization.

LFIs must ensure that all relevant information relating to STRs, SARs, and other report types is kept confidential, with due regard to the conditions and exceptions provided for in the law, and the guiding principles for this must be established in policies and procedures. LFIs should ensure that policy and procedures are reflected in for example, appropriate access rights with regard to core systems used for case management and notifications, secure information flows and guidance/training to all employees involved. This guidance and training are particularly important for the first line of defense employees who have contact with customers. It is essential that these employees know when there may be cases of suspicious transactions, what questions they have to ask the customer and which information they must not under any circumstances disclose to the customer.

It should be noted that the confidentiality requirement **does not pertain** to communication within the LFIs or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to money laundering and the financing of terrorism and illegal organisations, according to the Article 39.1 of the AML-CFT Decision.

It is a federal crime for LFIs or their managers, employees, or representatives, to inform a customer or any other person, whether directly or indirectly, that a report has been filed or will be filed, or of any information or data contained in the report, or that an investigation is under way concerning the transaction, otherwise known as "tipping off." Any person violating this prohibition is liable to a penalty of no less than AED100,000 and no more than AED500,000 and imprisonment for a term of not less than six months, according to the Article 25 of the AML-CFT Law.

6. Handling of Transactions and Business Relationships after Filing STRs or SARs

6.1. Requirements for Corresponding with the FIU

As a standard practice and as specified in Article 9.1 of the AML-CFT Law, the FIU can reach out to LFIs to provide additional requested information pertaining to an STR or SAR. Therefore, when responding to the FIU's inquiries, details should be provided in a way that is precise and outlined as per the request. LFIs

should maintain clarity on the presented information and provide it in the required format (e.g., tabular format, pdf, etc.). Moreover, LFIs should avoid adding unnecessary codes and abbreviations or any raw information extracted directly from the core databases, which are unknown to the FIU. It is important to understand that the details pertaining to the source and destination of funds are essential for investigating the reported activity. Therefore, names; account numbers; country of origin and destination; currencies; dates; source and purpose of transactions; and other related information should be detailed in LFI's response. Once the report is filed, LFI should send the report web reference number and inform the FIU via the goAML Message Board.

6.2. Post STR and SAR Process

Following an STR or SAR filing, the FIU may or may not revert to the LFI with specific instructions, requests for additional information, feedback or further guidance related to the STR or SAR, or to the business relationship in general. In such cases, these communications will generally be directed to the Compliance Officer or MLRO of the LFI. However, LFIs may not receive instructions, additional information requests, or other feedback from the FIU regarding STRs or SARs that have been filed; or the receipt of such communications may be delayed beyond what they consider to be a reasonable time period. In such instances, LFIs must follow their internal policies in relation to such customers and should determine the appropriate handling of the STR or SAR and of the business relationship in general, taking into consideration all of the risk factors involved.

Specifically, once a suspicious transaction or other suspicious information related to a customer or business relationship has been reported to the FIU, the LFI should take the following immediate responses:

- LFIs should follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general.
- LFIs should identify all related/associated accounts or relationship of STR or SAR customers and conduct a review on those accounts/relationship to check whether any suspicious transaction(s) has taken place. If yes, appropriate risk-based Enhanced Due Diligence ("EDD") and ongoing monitoring procedures should be implemented.
- The customer or business relationship, including the related/associated accounts and relationship to the STR or SAR customers, should immediately be classified as a high-risk customer and appropriate risk-based EDD and ongoing monitoring procedures should be implemented in order to mitigate the associated money laundering and the financing of terrorism and illegal organisations risks.

Unless specifically instructed by the FIU to do so, LFIs are under **no obligation** to carry out transactions they suspect, or have reasonable grounds to suspect, of being related to a crime. Furthermore, unless specifically instructed by the FIU to maintain the business relationship (for example, so that the competent authorities may monitor the customer's activity), it should be the LFI's responsibility to take appropriate steps in order to decide whether or not to maintain the business relationship based on their risk appetite. However, LFIs should consider the risk of tipping off a customer when taking these restrictive measures on the account. These steps may include, but are not limited to:

- Reassessing the business relationship risk and re-evaluating the customer's risk profile, where necessary.

- Initiating an enhanced customer due diligence review.
- Considering the performance of an enhanced background investigation (including, if appropriate, the use of a third-party investigation service).
- Any other reasonable steps, commensurate with the nature and size of their businesses, and bearing in mind the obligation to avoid "tipping off" the customer.

LFIs that determine to maintain the business relationship should, commensurate with the nature and size of their businesses:

- Document the process by which the decision was made to maintain the business relationship, along with the rationale for, and any conditions related to, the decision; and
- Implement adequate EDD measures to manage and mitigate the money laundering/the financing of terrorism and illegal organisations risks associated with the business relationship.

In such cases, beyond EDD measures, LFIs should also implement additional control measures such as, but not limited to:

- Requiring additional data, information or documents from the customer in order to carry out transactions (for example, evidence of relevant licenses or authorizations, customs documents, additional identification documents, bank or other references).
- Restricting the customer's use of certain products or services.
  Placing restrictions and/or additional approval requirements on the processing of the customer's transactions (for example, transaction size and/or volume limits, or limits to the number of transactions of certain types that can be executed during a given time period).

LFIs should also document the specific EDD, ongoing monitoring, and additional control measures to be taken. In this regard, LFIs should obtain senior management approval for the plan, including its specific conditions, duration and any requirements for its removal, as well as the roles and responsibilities for its implementation, monitoring and reporting, commensurate with the nature and degree of the money laundering and the financing of terrorism and illegal organisations risks associated with the business relationship.

Thus, retaining a customer relationship, exiting the relationship, restricting an account, or any other actions taken by an LFI following the filing of an STR, SAR, or other report is a decision based on the LFI's internal policies and procedures, including its risk appetite, to safeguard the LFI from relevant risks. This is unless the entity receives instructions from the FIU or any other competent authority that should be immediately implemented without delay. In cases where the LFI decides to reject a new customer or to exit an existing relationship due to an STR or SAR filing (or other report), the LFI should ensure that the subject of the filing is added to internal watch lists, (e.g., a list of individuals and entities that have been exited for financial crime-related reasons and that should be screened by the LFI to avoid future on-boarding).

While individual STRs, SARs, or other reports that pose particular risk may require escalation and review for potential exit, repeated filings on a single account or group of related accounts should trigger consideration of customer exit. Repeat filings should also prompt a review of risks associated with accounts of a similar type and of whether internal controls are effectively mitigating risk. An LFI should determine a threshold for which an account that has been subject to a certain amount of STR or SAR filings (or other

report) will be escalated to senior management for consideration of account closure, possible restrictions on the account, and/or enhanced monitoring.

LFIs should also maintain a customer exit policy that outlines the process for reviewing the overall customer relationship and deciding on next steps, including ending the relationship and notifying law enforcement and/or other group affiliates, as appropriate. Customer exit policies should include criteria for when these actions are appropriate and outline how the LFI should monitor the activity of a customer it decides to retain. The LFI should contact law enforcement before closing an account if the entity has knowledge of an ongoing law enforcement investigation involving that account or customer, or the LFI has filed an STR(s), SAR(s), or other report types on the customer or account due to continuing suspicious activity. LFIs should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that an LFI keep a particular account open, the LFI should ask for a written request. The written request should indicate that the agency has requested that the LFI maintain the account along with the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by an LFI in accordance with its own standards and guidelines.

6.3. Governance and Reporting to Senior Management

LFIs should have mechanisms to inform the Board of Directors (or a committee of the Board) and senior management of compliance initiatives, compliance deficiencies, STRs, SARs, or other regulatory reports filed, and corrective actions taken. LFIs should also develop and maintain a system of reporting that provides accurate and timely information on the status of the AML/CFT program, including statistics on key elements of the program, such as the number of transactions monitored, alerts generated, cases created, and STRs, SARs, or other report types filed.

Employees should report the number and types of STRs, SARs, or other regulatory reports filed to the Board of Directors or a Board-designated committee. While employees are not required to provide actual copies of STRs, SARs, or other regulatory reports to the Board (or a committee of the Board), such notifications should contain sufficient information to enable the Board or its committee to provide appropriate oversight over the LFI's AML/CFT program. Where an individual filing documents activity that poses a particular risk, management may provide a copy of the report to the Board or Board-designated committee. Where appropriate, the suspicious activity or transaction underlying the filing of an STR, SAR, or other regulatory reports should be communicated to those individuals responsible for managing the risk associated with the customer and/or activity that is the subject of the STR, SAR, or other regulatory reports in order to permit such employees to respond appropriately to the AML/CFT risks identified. Although all such communications are subject to the confidentiality restrictions, it should be noted that the confidentiality requirement does not pertain to communication within the LFIs or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention, or reporting of suspicious transactions and/or crimes related to money laundering and the financing of terrorism and illegal organisations, according to Article 39.1 of the AML-CFT Decision (also referenced in Section 5. Confidentiality and Prohibition against "Tipping Off").

6.4. Record Retention

According to Article 24 of the AML-CFT Decision, LFIs are required to retain all records and documents pertaining to STRs and the results of all analysis or investigations performed for at least five (5) years from the date of completion of the transaction or termination of the business relationship. Such records relate to both internal STRs and those filed with the FIU, and should include but are not limited to:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence;
- Competent authority request for information, correspondent bank requests for assistance, and their related investigation files and correspondence;
- CDD and Business Relationship monitoring records, documents, and information obtained in the course of analyzing or investigating potentially suspicious transactions, requests for assistance by LFIs, and all internal or external correspondence or communication records associated with them;
- STRs, SARs, and other report types (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records, and all related correspondence; and
- Notes concerning feedback provided by the FIU with respect to reported STRs, SARs, and other report types, as well as notes or records pertaining to any other actions taken by, or requested by, the FIU.

Annex 1. Indicative Examples of Insufficient STR and SAR Narratives

Example 1:

- Reason for reporting: Statements show large payments to luxury car companies. High amounts of funds transfers continue over several months.

Comments: The narrative lacks identifying information on the STR subject (name, occupation, address, account number, etc.), and no explanation is given as to why the LFI considers this activity suspicious. The narrative lacks specific transaction data that identifies the dates and amounts of the large payments and specific details on the destination of the funds (the name, location, bank, and account number of the beneficiary car companies, if identifiable).

Example 2:

- Money orders were purchased on 03-28-21 to ABC Corporation in the amount of AED30,000.

Comments: No explanation is given as to why the MVTS considers this activity suspicious. The LFI does not indicate if money orders were purchased with cash. The LFI does not provide any information about the purchaser or nature of the business (ABC Corporation) and if this activity was normal or unusual for the purchaser or the business.

Example 3:

- Mr. X was the originator of 12 wires totaling AED400,000. All of the wires were remitted to a Hong Kong based company. During the same period of time, Mr. X deposited cash into his account.

Comments: The narrative lacks specific details on the destination of the funds (the name of the Hong Kong based company, bank, and account number of the beneficiary, if identifiable). The depository LFI fails to include any information concerning the relationship, if any, between the LFI and the customer. Also, no specific transaction data is provided that identifies the dates and amounts of each wire transfer and the cash deposit.

Example 4:

- The reason for the suspicion is due to multiple third-party transfers being paid into Mr. Y account that were soon followed by multiple cash withdrawals. Funds sent from the account to multiple third parties.

Comments: The narrative lacks specific details on the source of the funds (the individual/entity sending the multiple third-party transfers). The STR does not provide a timeframe of when the transfers were made, the number and value of the third-party transfers, the number and value of the cash withdrawals, and the timeframe (how soon) the cash withdrawals were made following the third-party transfers. The depository LFI fails to include any information concerning the relationship, if any, between the individual/entity sending the multiple third-party transfers and the customer.

Example 5:

- Information has come to our attention that the Mrs. Y has been convicted of a drug trafficking offense.

Comments: The narrative fails to describe the depository LFI's relationship with the subject and include additional identifying details about the subject (name, occupation, address, account number, etc.). The narrative does not describe any suspicious activity aside from the conviction and fails to state if the suspicion is related to money laundering or if there are possible links to the financing of terrorism and illegal organisations.

Example 6:

- Mrs. Y came into the bank and asked questions during the account opening process that were suspicious.

Comments: The narrative does not describe the suspicious activity in detail as a basis for filing the SAR (e.g., the customer refusing to answer account opening questions; providing falsified or counterfeit documentation; exhibiting reluctance to provide detailed information about the customer's business). The narrative template also fails to describe information that the LFI was able to gather on the prospective customer during account opening (occupation, address, etc.).

Example 7:

- Mr. LMN was the subject of adverse media involving his association with a terrorist group.

Comments: The narrative fails to describe the depository LFI's relationship with the subject and include additional identifying details about the subject (name, occupation, address, account number, etc.). The narrative template also does not identify the terrorist group, describe the customer's relationship with the terrorist group, the timeframe for the customer's involvement with the terrorist group, and how the LFI became aware of this association, such as a hyperlink to the adverse media report.

Example 8:

- Mrs. ABC purchased an insurance product using unusual payment methods. Mrs. ABC is a teacher at Happy Day Elementary School in Dubai and resides at 11111 Street Name, Dubai, UAE. Mrs. ABC also has two motor vehicles insured with the LFI since April 2019.

Comments: The narrative fails to describe the type of insurance product purchased, on what date, with what payment method, and why the institution considers this payment method unusual. The institution also does not indicate the customer's stated purpose for purchasing the insurance product and if this is line with what the LFI knows about the customer.

Example 9:

- Mr. XYZ requests to increase payments on his life insurance policy during the period from 02-01-21 to 05-01-21, and the payments appear to be excessive, given Mr. XYZ's prior history.

Comments: The narrative fails to include additional identifying details about the subject (name, occupation, address, etc.). The narrative lacks specific transaction data that identifies the dates, amounts, and method of payment on the life insurance policy. The narrative also does not describe why the institution considers these payments to be excessive based on the customer's prior history of payments. The narrative does not indicate how long the subject has been in possession of the life insurance policy.

Annex 2. Red Flag Indicators in the Context of the UAE

The FIU published the following typologies and indicators in their Biannual Financial Crime Trends and Typologies Report (January – June 2020). These typologies and indicators, as well as any future ones the FIU may determine, should be incorporated into an LFI's AML/CFT program with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.

B.1 General indicators

According to the FIU, the following indicators are present in many of the typologies used in money laundering and the financing of terrorism and illegal organisations.

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption.
- Significant and/or frequent transactions in contrast to known or expected business activity.
- Significant and/or frequent transactions in contrast to known employment status.
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds.
- Where relevant, nervous or uncooperative behavior exhibited by the LFI's employees and/or customers.

B.2 Wire transfers to and from bank accounts

- **How it works:** Transferring proceeds of crime from one person to another via money remittance services.
- **Possible indicators**
  - Significant and/or frequent cash payments for transfers.
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Transfers to high-risk countries or known tax havens.
  - Transfers to numerous offshore jurisdictions with no business rationale.
  - Same home address provided by multiple remitters.
  - Reluctant to provide the LFI with identification details.

B.3 Purchase of valuable commodities

- **How it works:** Laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.
- **Possible indicators**
  - Significant and/or frequent cash purchases of valuable commodities.
  - Regularly buying and selling of valuable commodities that is not supported with a business purpose and/or does not make economic sense.

B.4 Purchase of valuable assets

- **How it works:** Laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.
- **Possible indicators**
  - Purchase/sale of real estate above/below market value irrespective of economic disadvantage.
  - Cash purchases of valuable assets with cash and/or cash deposits for valuable assets.
  - Low value property purchased with improvements paid for in cash before reselling.
  - Rapid repayment of loans/mortgages with cash or funds from an unlikely source.

B.5 Offshore companies

- **How it works**: The process of registering companies in the UAE, especially in the free zones, with foreign directors and/or shareholders in order to open bank accounts to facilitate money laundering and/or the financing of terrorism and illegal organisations by unverified beneficiaries.
- **Possible indicators**
  - Large numbers of companies registered with the same office address.
  - Address on file is for a 'Virtual office'.
  - Accounts/facilities are opened/operated by company formation agents.
  - Lack of information regarding overseas directors/beneficiaries.
  - Complex ownership structures.
  - Companies where there is no apparent business purpose.
- **Additional indicators:**
  - The same natural person is the director for a large number of single director companies.
  - The same person (natural or corporate) is the shareholder of a large number of single-shareholder companies.
  - Use of a small number of local 'agents' who undertake transactions with the companies' register.

B.6 Nominees, trustees, family members or third parties

- **How it works:** Utilizing other people to carry out transactions in order to conceal the true identity of the individual ultimately controlling the proceeds of crime.
- **Possible indicators**
  - Customers using family members or third parties, including the use of children's accounts.
  - Transactions where third parties seem to be retaining a portion of funds, which would indicate the use of mules.
  - Accounts operated by someone other than the account holder.
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Significant and/or frequent transactions made over a short period of time.

B.7 Trade-based money laundering

- **How it works:** Manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.
- **Possible indicators**
  - Invoice value greater than value of goods.
  - Discrepancies in domestic and foreign import/export data.
  - Suspicious cargo movements.
  - Suspicious domestic import data.
  - Discrepancies in information regarding the origin, description, and value of the goods.
  - Discrepancies with tax declarations on export declarations.
  - Sudden increase in online auction sales by particular vendors (online auction sites).
  - Frequent purchases between same buyers and vendors (online auction sites).

B.8 Cancellation of credits or overpayments

- **How it works:** Laundering proceeds of crime by overpaying then requesting refund cheques for the balance.

- **Possible indicators**
  - Frequent cheque deposits issued by car dealers, dealers in jewelry, etc.
  - Significant and/or frequent payments to utility companies, for example, prepaid cards for fuel, telecom e-wallets etc.
  - Frequent cheque deposits issued by utility companies (i.e., electricity providers).
  - Significant and/or frequent payments for purchases from online auction sites.
  - Frequent personal cheque deposits issued by third parties.

B.9 Electronic transfers to and from bank accounts

- **How it works:** Transferring proceeds of crime from one bank account to another via LFIs.
- **Possible indicators**
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Transfers involving accounts located in high-risk countries or known tax havens.
  - Transfers to offshore jurisdictions with no business rationale.
  - Multiple transfers sent to the same person overseas by different people.
  - Departure from the UAE shortly after transferring funds.
  - Transfers of funds between various accounts that show no economic purpose (i.e., multiple transfers incurring bank fees where one single transfer would have been sufficient).

B.10 Co-Mingling

- **How it works:** Combining proceeds of crime with legitimate business takings.
- **Possible indicators**
  - Significant and/or frequent cash deposits when business has electronic funds transfer at point-of-sale facilities.
  - Large number of accounts held by a customer with the same LFI.
  - Accounts operated by someone other than the account holder.
  - Merging businesses to create layers.
  - Complex ownership structures.
  - Regular use of third-party accounts.

B.11 Gatekeepers/professional services

- **How it works:** Utilizing 'Professionals' to establish seemingly legitimate business activities, for example, Lawyers, Accountants, Brokers, Company Formation Agents.
- **Possible indicators**
  - Accounts and/or facilities opened and/or operated by company formation agents.
  - Gatekeepers that appear to have full control.
  - Known or suspected corrupt professionals offering services to criminal entities.
  - Accounts operated by someone other than the account holder.

B.12 Cash deposits

- **How it works:** Placement of cash into the financial system.
- **Possible indicators**
  - Large cash deposits followed immediately by withdrawals or electronic transfers.

B.13 Structuring

- **How it works:** Separating large transactions into small transactions to avoid scrutiny and detection from LFIs.
- **Possible indicators**
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Small/frequent cash deposits, withdrawals, electronic transfers made over a short time period.
  - Multiple low value domestic or international transfer.

B.14 Smurfing

- **How it works:** Utilizing third parties or groups of people to carry out structuring.
- **Possible indicators**
  - Third parties conducting numerous transactions on behalf of other individuals.
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Accounts operated by someone other than the account holder.

B.15 Credit Cards/Cheques/Promissory Notes

- **How it works:** Instruments used to access funds held in an LFI, often in another jurisdiction.
- **Possible indicators**
  - Frequent cheque deposits in contrast to known or expected business activity.
  - Multiple cash advances on credit card facilities.
  - Credit cards with large credit balances.

B.16 Transactions inconsistent with intended purpose of the account

- **How it works:** Transactions that are out of the ordinary for the individual or conducted without a clear rationale.
- **Possible indicators**
  - Transactions to or from unrelated parties.
  - Transaction amounts that are inconsistent with the account's expected volumes or frequencies.
  - Transactions that are out of the ordinary for the customer's profession or business activity.

B.17 Cash couriers

- **How it works**: Concealing the movement of currency from one jurisdiction to another using people, luggage, mail, or any other mode of shipment, without declaration.
- **Possible indicators**
  - Transactions involving locations with poor AML/CFT regimes or high exposure to corruption.
  - Customers originating from locations with poor AML/CFT regimes/high exposure to corruption.
  - Significant and/or frequent cash deposits made over a short period of time.
  - Significant and/or frequent currency exchanges made over a short period of time.

B.18 Other payment technologies

- **How it works**: Utilizing emerging or new payment technologies such as virtual currencies/crypto-currencies, peer-to-peer (P2P) lending etc. to facilitate money laundering and/or the financing of terrorism and illegal organisations.

- **Possible indicators**
  - Excessive use of stored value cards.
  - Significant and/or frequent transactions using mobile telephone services.
  - Unjustified transactions to and from Cryptocurrency platforms and digital assets exchanges.

B.19 Underground banking/alternative remittance services

- **How it works**: Transferring proceeds of crime from one person to another via informal banking mechanisms such as unregistered Hawaladars.
- **Possible indicators**
  - Mostly prevalent under the auspices of a general trading company license.
  - Significant and/or frequent cash payments for transfers in which the cash deposits could be from many different individuals using the cash deposit machines.
  - Cash volumes and transfers in excess of average income of migrant account holders.
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Large transfers from accounts to potential cash pooling accounts.
  - Significant and/or frequent transfers recorded informally using unconventional book-keeping.
  - Significant and/or frequent transfers requested by unknown or intermittent customers.
  - Numerous deposits to one account followed by numerous payments made to various people.
  - Vague invoices and documentation which may deliberately be made to appear complex.

B.20 Cash exchanges

- **How it works**: Exchanging low denomination notes for high denomination notes (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **Possible indicators**
  - Significant and/or frequent cash exchanges from small to large denominations.

B.21 Currency conversion

- **How it works:** Converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **Possible indicators**
  - Significant and/or frequent local or foreign currency exchanges.
  - Opening of foreign currency accounts with no apparent business or economic purpose.

Annex 3. Red Flag Indicators for the UAE Insurance Sector

The UAE Insurance Authority has issued the following list of red flag indicators when handling life and general insurance products. The indicators, as well as any future ones the UAE Insurance Authority may determine, should be incorporated into an LFI's AML/CFT program with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity related to life and general insurance products.

1. The purchase of an insurance product does not reflect a customer's known needs (e.g., purpose of the account).
2. The early surrender of an insurance product is taken at a cost to the customer.
3. The surrender of an insurance product is initiated with the refund directed to a third party.
4. The customer exhibits no concern for the investment performance of a purchased insurance product and instead exhibits significant concern for its early surrender terms.
5. The customer purchases insurance products using unusual payment methods, such as cash or cash equivalents, or with monetary instruments in structured amounts.
6. The customer demonstrates reluctance to provide identifying information when purchasing an insurance product.
7. The customer borrows the maximum amount available from their insurance product shortly after purchase.
8. The customer used to purchase low-premium insurance and pay premiums by making regular payments but suddenly purchases insurance that requires a large lump-sum premium payment, for which no reasonable explanations are provided.
9. The customer purchases an insurance product without concern for the coverage or benefits, or the customer only cares about the procedures for the policy loan, cancellation of insurance policy, or changing beneficiary when purchasing an insurance policy that has a high cash value or requires a high lump-sum premium payment.
10. The customer usually pays a premium by making regular payments but suddenly requests to purchase a large-sum policy by paying off premium all at once.
11. The customer purchases insurance products with high cash value successively over a short period of time, and the insurance products purchased do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
12. The customer pays premiums in cash and in several payments marginally below the threshold for declaration but cannot reasonably explain the source of funds. In addition, the transactions do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
13. The customer, after making a large premium payment for a policy purchased, applies for a large policy loan or cancels the policy in a short period of time, for which no reasonable explanations are provided.
14. The customer is a policyholder of several motor vehicles which is inconsistent with their profile.
15. The theft of a motor vehicle is not reported by the customer/policyholder.
16. The customer attempts to insure a motor vehicle that was reported as stolen or as a total loss.

Annex 4. Overarching Rules and Principles for the goAML System

The FIU published the goAML XML Submission Guide (please see Section 3.4) with additional detail on the rules that an LFI should consider when submitting an STR, SAR, or other report type in the goAML system:

- All LFIs transactions should be reported as bi-party transactions on the goAML system.
- Reporting entities should submit only suspicious transactions in a report. Any additional transactions can be submitted via an AIFT (upon request only).
- For AIFT submissions where the number of transactions exceed 10,000, reporting entities are advised to split them into more than one AIFT; however, the AIFT should use the same "Internal Reference Number".
- A deposit is composed of a bi-party transaction occurring from a person who may be a conductor to an account.
- A withdrawal is composed of a bi-party transaction occurring from an account to a person.
- A remittance is composed of a bi-party transaction occurring from one person/account/entity to another.
- A wire transfer is composed of a bi-party transaction occurring from an account to another account.
- In case a LFI is acting as a correspondent bank within a reported transaction, then the transaction is occurring from one account to another, in which both accounts should be classified as 'Not My Client' by the LFI/Compliance Officer/MLRO.
- In the case of Exchange Houses, where a currency exchange transaction is being reported, it should be reported as a bi-party transaction, where the "from" and "to" parties are the same Person.
- The conductor field is mandatory when the transaction is conducted from an entity.
- If the date of birth for a subject (person) is unknown, then the user may enter the 1st of January 1900 in the 'Birth Date' field.
- In case the expiration date of a registered ID is unknown, then the user may enter the 31st of December 2100 in the 'Expiry Date' field.
- When reporting a transaction that involves an account, it is imperative that the LFI also provide details for the person or entity associated with the said account.

Annex 5. Synopsis of the Guidance

Introduction	Purpose	The purpose of the 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.
	Applicability	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.
	Legal Basis	The legal basis of STR reporting is based on the (i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering (AML) and Combatting the Financing of Terrorism (CFT) and Financing Illegal Organisations; (ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations; and (iii) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution. The legal basis addresses (i) the consequences for failure to disclose suspicious activity, (ii) protection for individuals disclosing suspicious activity, and (iii) the meaning of suspicious transactions.
Identification of Suspicious Transactions	Role of the First Line of Defense	The first line of defense plays a critical role in the management of customer and third-party risk and the timely escalation of potentially suspicious activity. The first line of defense is well-placed to identify suspicious transactions and assess that information once deemed reasonable—collected through interactions with a customer—now appears suspicious. Employees within the first line of defense include relationship managers, business executives, and back-office operations functions.
	Role of the Second Line of Defense	The second line of defense (e.g., compliance employees) provides policy, advice, guidance, assurance, oversight, and challenge to the first line of defense. While employees in Financial Crime Operations Units (possibly in the first line of defense) can investigate suspicious transactions and document the resultant investigation, the ultimate filing of the STR or SAR should be made by the Compliance Officer or the money laundering reporting officer (MLRO) (in the second line of defense). The second line of defense is charged with overseeing the investigations programme.
	Role of the Third Line of Defense	The third line of defense identifies gaps, deficiencies, and weaknesses in operational controls owned or overseen by an LFI's business, operations, and compliance functions.
	Purpose of Transaction Monitoring	The purpose of transaction monitoring is the ongoing, retrospective monitoring of customers' and prospective customers' transactions or activity to identify activity anomalous from normal behavior. This may, on further investigation, generate knowledge or reasonable suspicion of financial crime and thereby require reporting to the appropriate law enforcement and/or regulatory authority as an STR, SAR, or equivalent local report in line with AML/CFT regulatory and/or UAE FIU reporting requirements.
	Internal Organization	An LFI's internal organization is important to appropriately identify unusual or potentially suspicious activity. Internal organization comprises an LFI's governance and management oversight; policies and procedures; clear lines of responsibility and reporting; and ongoing training to account for changes in the UAE's legislative and regulatory frameworks. There are also specific considerations for institutions with foreign branches and subsidiaries.
	Transaction Monitoring Methods	A transaction monitoring program should take into account the AML/CFT risks of the LFI's customers, prospective customers, counterparties, businesses, products, services, delivery channels, and geographic markets in addition to helping prioritize high-risk alerts. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or a combination of these, including an intelligence-led transaction monitoring approach.

Procedures for the Reporting of Suspicious Transactions	Importance of Filing an STR or SAR	Information generated from an STR, SAR, and other report type is important for law enforcement and the FIU to effectively identify and combat financial crime. Specifically, the quality of STRs, SARs, and other report types is imperative for increasing the FIU's analytical function to identify vulnerabilities and threats to the UAE financial system and develop an overall understanding of money laundering and the financing of terrorism and illegal organisations risks.
	Basic Structure of an STR or SAR	Different report types can be filed in the FIU's "goAML" portal (i.e., STR, SAR, AIF, AIFT, RFI, RFIT, HRC, HRCA). In addition, an LFI should divide a narrative into three sections (introduction, body, and conclusion).
	Best Practices for Drafting an STR or SAR	A narrative should identify and answer the five questions – who? what? when? where? and why? – of the suspicious activity being reported to the FIU in addition to the operation/modus operandi (or how?). The Guidance also addresses how defensive STR or SAR filings are generally discouraged.
	How to Submit an STR or SAR	LFIs are required to submit suspicious transaction and activity reports directly to the FIU using the "goAML" portal. There are certain mandatory fields that an LFI should populate when submitting a report in the goAML portal in addition to providing certain supplemental documents.
	Amendments to Submitted Reports	Once a report is submitted and accepted in the goAML system, changes cannot be applied, including amendments for missing or incorrect information. However, LFIs may file a corresponding AIF, AIFT, RFI, or RFIT.
Timing of Alert Reviews and STR Filings	Alert Review, Case Investigation, and STR or SAR Decision Making	Within 20 days of alert generation, LFIs are expected to (i) review an alert and determine whether further investigation is warranted; (ii) conduct an investigation of the alerted activity and make a recommendation as to whether an STR or SAR should be filed; and (iii) make a determination on whether the activity is suspicious and requires an STR or SAR (based on the Compliance Officer or MLRO's determination).
	STR or SAR Filing	In the absence of escalation for expedited review, the Compliance Officer or MLRO should file an STR or SAR to the FIU within 15 days from the date of determining that a transaction meets the definition of suspicious activity. In the event of escalation for expedited review, the Compliance Officer or MLRO should file an STR or SAR to the FIU within 24 hours of the determination.
	Monitoring and Reporting of Continuing Suspicious Activity	Any new activity involving a previous STR or SAR subject should be reviewed within 90 days of the last reported transaction. Where such a review uncovers continuing suspicious activity, the LFI should file an STR or SAR within 105 days from the date of the previous STR or SAR filing. A 'post-STR or SAR' review can be achieved either manually or via an LFIs' automated and ongoing transaction monitoring systems/scenarios.
	Activity Requiring Immediate Attention	Situations requiring immediate attention include reportable violations that are ongoing (e.g., part of an ongoing money laundering scheme as indicated by an appropriate law enforcement authority) and transactions that the LFI suspects are related to the financing of terrorism and illegal organisations.
	Exceptions for Complex Investigations	There may be instances when the LFI encounters potentially unusual or suspicious activity that is of a "complex" nature. If the LFI designates an investigation as "complex," the LFI should submit an initial STR or SAR filing within 15 days of determination that the activity is suspicious. The LFI then has an additional 30 days to obtain all necessary information related to the complex investigation and submit a follow-up STR or SAR to the FIU. The FIU can approve additional extensions beyond 30 days on a case-by-case basis.
	Summary of Review, Investigation, and Reporting Timelines	There are recommended timelines for the review, investigation, and reporting of suspicious activity in the absence of an escalation for expedited review.
	Escalation for Expedited Review	In certain cases, an alert or case may need to be dispositioned and an STR or SAR filed more rapidly than usual processes allow. In such cases, the alert will be dispositioned and the STR or SAR filed within 24 hours.

Confidentiality and Prohibition against "Tipping Off"	Confidentiality and Prohibition against "Tipping Off"	When reporting suspicious activity or transactions to the FIU, LFIs are obliged to maintain confidentiality regarding both the information being reported and specific to the act of reporting itself, and to make reasonable efforts to ensure that the information and data reported are protected from access by any unauthorized person.
Handling of Transactions and Business Relationships after Filing STRs	Requirements for Corresponding with the FIU	If the FIU reaches out to an LFI for additional information pertaining to an STR or SAR, details should be provided in a way that is precise and outlined as per the request. LFIs should maintain clarity on the presented information and provide it in the expected format.
	Post STR or SAR Process	Following the filing of an STR or SAR filing, LFIs are obliged to follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general. LFIs may decide to retain a customer relationship, exit the relationship, or restrict an account, among others. Any actions taken by an LFI following the filing of an STR or SAR is a decision based on the LFI's internal policies and procedures, including its risk appetite, although LFIs should consider the risk of tipping off a customer when implementing such restrictive measures.
	Governance and Reporting to Senior Management	LFIs should have mechanisms to inform the Board of Directors (or a committee of the Board) and senior management on the status of its AML/CFT program, including reporting on the number and types of STRs or SARs.
	Record Retention	LFIs are required to retain all records and documents pertaining to STRs or SARs and the results of all analysis or investigations performed for a period of no less than five (5) years from the date of completion of the transaction or termination of the business relationship.
Annexes	Annex 1: Indicative Examples of Insufficient STR or SAR Narratives	Examples of insufficient STR or SAR narratives are provided with an explanation on why these STR or SAR narratives are not sufficient and comprehensive.
	Annex 2. Red Flag Indicators in the Context of the UAE	The FIU published typologies and indicators of suspicious activity that an LFI should consider with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.
	Annex 3. Red Flag Indicators for the UAE Insurance Sector	The UAE Insurance Authority issued a list of red flag indicators that an LFI should consider with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.
	Annex 4. Overarching Rules and Principles for the goAML System	The goAML XML Submission Guide provides additional detail on the rules that an LFI should consider when submitting an STR, SAR, or other report type in the goAML system.
	Annex 5	Synopsis of the Guidance

The following table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the absence of escalation for expedited review.

Action	Maximum Timeline in Calendar Days
Dispositioning of alert; recommendation on whether to file an STR or SAR; and decision on whether to file an STR or SAR	Within 20 days of alert generation
Filing of first STR or SAR	15 days from decision to file *(35 days from alert generation)*
Filing of a follow-up STR or SAR for a "complex investigation"*	30 days from first STR or SAR filing *(65 days from alert generation)*
Filing of STR or SAR on continuing activity	105 days from previous STR or SAR

In certain cases, an alert or case may need to be dispositioned and an STR or SAR filed more rapidly than usual processes allow. In such cases, the alert will be dispositioned and the STR or SAR filed according to the expedited review timeline as laid out below. Circumstances where expedited review is expected include:

- The **activity requires immediate attention**, including reportable violations are ongoing (e.g., part of an ongoing money laundering scheme as indicated by an appropriate law enforcement authority), or the LFI suspects transactions are related to the financing of terrorism and illegal organisations.
- The facts available at the alert review stage **are or may be sufficient to warrant a STR or SAR filing without further investigation**.

The following table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the event of escalation for expedited review.

Action	Maximum Timeline in Calendar Days
Decision on whether to file an STR or SAR and filing of first STR or SAR	24 hours from decision to file
Filing of STR or SAR on continuing activity	105 days from previous STR or SAR

**The following is a non-exhaustive list of factors that should be considered to determine whether investigated activity qualifies as a complex investigation: employee-related investigations; significant investigations involving multiple customers, multiple jurisdictions, multiple accounts, multiple transactions, and/or multiple subpoena requests; and legal referred investigations.*