



Suspicious Transactions Reports (STRs)

Guidance on Reporting

Addressed to reporting entities mentioned in articles 4 and 5 of AML/CFT Law no.44 dated November 24, 2015.

Contents

1. Introduction	3
2. Reporting Entities	4
2.1. Financial Institutions	4
2.2. Designated Non-Financial Businesses and Professions	4
3. Suspicious Transactions	5
3.1. Reasonable Grounds to Suspect	5
3.2. Completed or Attempted Transactions	6
4. STR Requirements	7
4.1. Time to Report	7
4.2. Methods of Submitting a STR	7
4.3. Information to be contained in the STR	8
5. Additional Information Related to Reporting	9
5.1. Confidentiality / Tipping-off	9
5.2. Immunity	9
5.3. Sanctions for Non-compliance	9
6. Examples of Common Indicators	10
6.1. General	10
6.2. Knowledge of Monitoring Procedures	11
6.3. Identity Documents	12
6.4. Cash Transactions	12
6.5. Economic Purpose	13
6.6. Customer's Accounts	13
6.7. Transactions Involving Areas Outside Lebanon	14
6.8. Transactions Related to Off-shore Business Activity	14

Reporting Suspicious Transactions to Special Investigation Commission- SIC

1. Introduction

This guidance is applicable to all reporting entities and is issued to assist the reporting entity “R.E.” to meet its reporting obligations of any transaction suspected to be related to money laundering and terrorism financing (ML/TF) under Law No. 44 of 2015 (AML/CFT Law). Suspicious transaction reports (STRs) play a crucial role in the fight against money laundering and terrorist financing, and the Special Investigation Commission (SIC) is committed to ensuring that Reporting Entities in Lebanon file suspicious transaction reports of the highest quality.

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering, associated predicate offences or terrorist financing. All references to suspicious transaction include a transaction that is either completed or attempted.

This guidance contains indicators of suspicious transactions that might be useful in helping “R.E.” assess whether a transaction is suspicious and should be reported. It is not intended as a substitute for “R.E.” own assessment, based on knowledge and experience as well as the specific circumstances of the transaction.

2. Reporting Entities

Under provisions of article 7 of Law No. 44 of 2015 (AML/CFT Law), Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPs), **must promptly report** to the SIC the details of operations undertaken or attempted to be undertaken that are suspected to be related to money laundering or terrorism financing. The following parties referred to in Articles 4 & 5 of AML/CFT Law are considered as reporting entities:

2.1. Financial Institutions

- Banks
- Financial Institutions
- Leasing Companies
- Institutions that perform money transfers electronically (also known as money remittance companies)
- Exchange Institutions (Category A & B)
- Financial Intermediation Institutions (also known as brokerage firms)
- Insurance companies
- Specialized Lending Entities (also known as Comptoirs)

2.2. Designated Non-Financial Businesses and Professions

- Casinos
- Real estate dealers and agents
- Merchants of Jewelry, precious stones and gold
- Lawyers
- Notaries
- Certified Accountants

Lawyers, Notaries and Certified Accountants must report STRs **if** a suspicion arise while preparing or carrying out on behalf of their customers any of the following activities:

- a. Buying and Selling of real estate
- b. Management of customer's movable and immovable assets, in particular transactions consisting of money accumulation and joint investment
- c. Management of bank accounts and securities accounts

- d. Organization of contributions for the establishment or management of companies
- e. Establishment or management of legal persons or unique legal arrangements, and buying and selling of single person enterprise or companies.

3. Suspicious Transactions

An unusual transaction whether **undertaken or attempted** to be undertaken may trigger **reasonable grounds to suspect** that it is related to money laundering or terrorist financing offence.

3.1. Reasonable Grounds to Suspect

Reasonable grounds to suspect will vary from one customer to another and from business to business, and the context in which the transaction occurs is a significant factor in assessing suspicion. The reasonable grounds to suspect may arise from red-flags such as the inconsistency with regard to the “R.E.” knowledge of the customer’s profile, from what they deem inappropriate behavior with regards to the line of legitimate business and financial history, or if the transaction does not make economic sense. Also a transaction may be considered as unusual in terms of its complexity, nature, volume and time of execution.

A transaction which appears unusual does not necessarily form reasonable grounds to suspect. Customers with a stable and predictable transaction profiles might have periodic unusual transactions or account activity. Therefore, **the unusual is, in the first instance, only a basis for further investigation**. On another note, a transaction with reasonable grounds to suspect may include several indicators where each one of them on its own seems irrelevant, but when linked together may raise suspicion.

Accordingly all circumstances surrounding a transaction or series of transactions should be assessed in order to properly determine the existence of reasonable grounds to suspect.

3.2. Completed or Attempted Transactions

The requirement for the “R.E.” to report a suspicious transaction applies if there is reasonable grounds to suspect, as explained in subsection 3.1. This applies not only when the financial transaction has been undertaken, but also when it has been attempted.

Completed transactions

A completed transaction is one that has occurred and was finalized. For example, if the “R.E.” processes a “financial transaction” from a customer for him to purchase an asset such as a life insurance policy or a real estate, then the financial transaction has occurred and is complete. This is true even if the final sale associated to the transaction does not materialize.

Attempted transactions

An attempted transaction is one that a customer intended to conduct and performed some form of action to do so. An attempted transaction is different from a simple request for information, such as an enquiry as to the fee applicable to a certain transaction. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either the “R.E.” or the customer.

The following are examples of attempted transactions:

- A financial institution or the casino refuses to accept a payment because the customer refuses to provide identification as requested.
- A brokerage firm refuses to process a transaction for which the customer insists on paying in cash because its business practice does not accept cash payments.
- A customer of a real estate agent starts to make an offer on the purchase of a house with a large payment, but will not finalize the offer once asked to provide identification.
- A customer requests from his accountant to facilitate a financial transaction involving large amount of cash. The accountant declines to conduct the transaction.

- A money remittance company declines to process a request to transfer a large amount of funds because the customer requesting the transfer refuses to provide identification.

4. STR Requirements

4.1. Time to Report

Once the “R.E.” has completed the measures that enabled it to determine that there is reasonable grounds to suspect that a financial transaction is related to an ML, associated predicate offence or TF, it **must promptly submit a STR to the SIC**. This applies to completed or attempted transactions, as explained in subsection 3.2. Reporting entities should ensure that their internal systems support the promptly filing of STRs and avoid unnecessary delay.

To note that there is no monetary threshold associated with the reporting of a suspicious transaction.

4.2. Methods of Submitting a STR

Parties referred to in Article 4 & 5 of Law 44

Reporting entities shall submit STRs electronically to the SIC using the required E-STR form along with all relevant documents. Reporting entities must submit by paper if unable to utilize technological capacity to send a STR electronically.

To report STRs electronically, the “R.E.” must be enrolled and logged in to the SIC web reporting system “**SEEDS**”, this application provides secure encrypted transmission that ensures the data's confidentiality and integrity.

To report STRs by paper, if (E-STR) is not available, the “R.E.” can print the STR form from the SIC website, fill it as PDF form or manually and send it in a sealed envelope on which the expression “**Strictly Confidential**” is clearly indicated. The envelope should be addressed to the SIC chairman or secretary-general.

Lawyers reporting mechanism

Lawyers shall report their suspicious transactions through the mechanism detailed in annex “C” of the “Lawyers’ AML/CFT obligations manual”, syndicate decision dated 20/4/2017.

(Refer to Lawyers obligations manual)

Feedback

The SIC shall send feedbacks to “R.E.” on the status of its filed STR and its quality. Moreover, the SIC statistics published in its annual report serves as guidance.

4.3. Information to be contained in the STR

It is essential that the “R.E.” complete all relevant fields in the STR form with as much accurate information as is available, with regards to reported individuals and/or entities involved in the transactions, information on the reported account or transactions, indicators of suspicion and suspected ML/TF predicate offense.

Reporting entities should clearly and to the extent available describe all of the factors or unusual circumstances that led to a suspicion of money laundering or terrorist financing activity, and provide as many relevant details as possible to support this determination to ensure STR quality, such as:

- Suspects involved along with details on their full names and CDD information
- Information on the suspected ML/TF offense
- Detailed business activity description of natural &/or legal persons that are subject of the STR
- Information on previously filed STRs related to natural &/or legal persons that are the subject of the new STR
- Information on suspicious transactions and suspicious business relations
- Detailed description of ML/TF scheme applied by suspicious natural &/or legal persons.
- Information on the funds frozen in accordance with SIC decision / UN Security Council 1267- 1373.

To note that STRs filed with incomplete information might result in delay and entitles SIC requesting the missing information.

5. Additional Information Related to Reporting

5.1. Confidentiality / Tipping-off

Reporting entities, as well as their board members, officers and employees, are prohibited from disclosing or insinuating to anyone that a suspicious transaction report or other relevant information is submitted or intended to be submitted to the SIC or that the SIC is inquiring about customers or auditing their operations or accounts.

(Article 11 of AML/CFT Law)

Reporting entities may continue dealing with the customers normally and in accordance with the rules, as long as the SIC does not issue a decision to the contrary.

5.2. Immunity

Reporting entities and their staff, shall enjoy immunity. Thus they may not be prosecuted or sued, neither collectively nor individually, for any civil or criminal liability related to the performance of their duties under the provisions of AML/CFT Law or according to the decisions of the SIC, particularly when they report in good faith to the SIC the details of operations they suspect to be related to money laundering or terrorism financing.

(Article 12 of AML/CFT Law)

5.3. Sanctions for Non-compliance

Reporting entities shall be subject to sanctions if they fail to meet the suspicious transactions reporting and tipping-off obligations. Failure to report a suspicious transaction could be punishable by imprisonment for a period of two months to one year and by a fine not exceeding one hundred million Lebanese pounds or by either penalties, also by administrative sanctions issued by their relative supervisory authority.

(Article 13 of AML/CFT Law)

6. Examples of Common Indicators

The following are examples of common indicators that may point to reasonable grounds to suspect money laundering or terrorist financing activity, whether undertaken or attempted as explained in subsection 3.2. Many of the situations described in these examples would be reasonably normal in some business contexts, whereas in others they would seem suspicious.

It should be noted, that the existence of a single indicator is not necessarily indicative of reasonable grounds to suspect. Therefore, analyzing the presence of one or more indicators, assessing the context in which the transaction occurs or is attempted, as well as knowledge of the customers' business and financial affairs will help identifying suspicious transactions.

These indicators are not intended to cover every possible situation and shall be viewed also in conjunction with other indicators including in prevailing BDL and SIC circulars as applicable. Reporting entities can identify suspicious transactions based on other criteria or known ML/TF indicators.

6.1. General

- Customer admits or makes statements about involvement in criminal activities.
- Customer does not provide a detailed home address.
- Customer appears to have accounts with several financial institutions in the same area for no apparent reason.
- Customer opens an account at a branch far from his residence or work.
- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Customer conducts his transactions at a branch different than his home branch.
- Customer repeatedly uses an address but frequently changes the names involved.
- Customer is accompanied to "R.E." premises and watched.
- Customer shows uncommon curiosity about internal control systems, and policies.
- Customer has only vague knowledge of the amount of a deposit.

- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer over justifies or explains the transaction.
- Customer is secretive and reluctant to meet in person.
- Customer is nervous, while executing the transaction.
- Customer's home or business telephone is invalid when an attempt is made to contact the customer shortly after initiating the business.
- Difficulty in verifying the background of a new or prospective customer.
- Customer appears to be acting on behalf of a third party, but does not tell you.
- Customer insists that a transaction be done quickly.
- Inconsistencies appear in the customer's presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client.
- Customer attempts to develop close relation with staff.
- Customer uses aliases and a variety of similar but different addresses.
- Customer spells his or her name differently from one transaction to another.
- Customer provides false information or information that you believe is unreliable.
- Customer offers you money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- You are aware or you become aware that a Customer is the subject of a money laundering or terrorist financing investigation or involved in illegal activities.
- A new or prospective customer is known to you as having a questionable legal reputation or criminal background.

6.2. Knowledge of Monitoring Procedures

- Customer attempts to persuade the "R.E." not to complete any documentation required for the transaction.
- Customer has known or makes inquiries that would indicate a desire to avoid reporting STRs.
- Customer seems very familiar with money laundering or terrorist financing issues.

6.3. Identity Documents

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce all identification documents requested.
- Customer only submits copies and not original personal identification documents.
- Customer exceedingly delays presenting corporate documents.
- All identification documents presented appear new or have recent issuance dates.
- Customer alters the transaction after being asked for identity documents.
- Customer presents different identification documents each time a transaction is conducted.

6.4. Cash Transactions

- Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.
- Customer frequently exchanges small bills for large ones.
- Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.
- Customer deposits extremely dirty bills.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Customer consistently deposits cash below the reporting threshold in an apparent attempt to avoid triggering the identification requirements.
- Customer presents uncounted funds for a transaction. Upon counting, the customer reduces the transaction to an amount just below the identification requirements.
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.

6.5. Economic Purpose

- Transaction seems to have no economic rationale or legitimate purpose, especially when there is a discrepancy between the transaction and the customer's occupation, or even between the transaction and the customer's financial profile.
- Transaction appears to be out of the normal course for industry practice.
- Transaction is carried out in exceptionally complicated circumstances.
- No business explanation for size of transactions or cash volumes.
- No clear financial connections between various businesses (i.e. a food exporter dealing with an automobile parts importer).

6.6. Customer's Accounts

- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Customer frequently uses many deposit locations outside of the home branch location.
- Opening accounts with names very close to other established business entities.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Large transfers from one account to other accounts that appear to be pooling money from different sources.
- Multiple deposits are made to a client's account by third parties.
- Unusually large cash deposits by a customer with personal or business links to an area associated with drug trafficking.

6.7. Transactions Involving Areas Outside Lebanon

- Customer and other parties involved in the transaction have no apparent ties to Lebanon.
- Transaction crosses many international jurisdictions.
- Cash volumes and international remittances in excess of average income for a migrant worker.
- Transaction involves high-volume international transfers to third party accounts in countries that are not usual remittance corridors.
- Transaction involves a country known for highly secretive banking law.
- The business relationship or the transaction involves countries that FATF has called to perform enhanced due diligence measures towards it.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.

6.8. Transactions Related to Off-shore Business Activity

- Accumulation of large balances, inconsistent with the known turnover of the client's business, and subsequent transfers to overseas account(s).
- Loans secured by obligations from offshore banks.
- Loans to/from offshore companies.
- Transactions involving an offshore “shell” bank whose name may be very similar to the name of a major legitimate institution.
- Use of letter-of-credit and other method of trade finance to move money between countries when such trade is inconsistent with the client's business.