GUIDANCE NOTE

REPORTING OBLIGATIONS FOR EXCHANGE COMPANIES IN KUWAIT ON SUSPICIONS OF MONEY LAUNDERING OR TERRORIST FINANCING

MAY 2025

1 INTRODUCTION

1.1 It is important to protect Kuwait against both money laundering, terrorist financing, and proliferation financing. Such types of crime can undermine the economic stability and security of the country, given that these crimes are supportive of organised crime and terrorism, and they weaken the integrity of the Kuwaiti financial system and other important businesses and professions. Exchange companies play an important role in protecting Kuwait against these kinds of crimes.

1.2 Exchange companies covered by the legislation on money laundering and terrorist financing

1.3 Exchange companies are covered by law no. 106 of 2013 on Anti-Money Laundering and Combatting the Financing of Terrorism. In Kuwait exchange companies are registered with the Central Bank of Kuwait (CBK), and are permitted to conduct both currency exchange and transfers of money.

1.4 Law no. 106 of 2013 mentions both currency exchange and money or value transfers in the listing of activities carried out by "financial institutions" that are comprised by the law:

"Any person who conducts as a business one or more of the following activities or operations for or on behalf of a customer on the following manner:

..

d. Money or value transfer services

..

h. Foreign exchange transactions,

.."

1.5 What is money laundering?

1.6 Money laundering is the process of disguising the origins of illegally obtained assets, including money, to make it appear as though it comes from legitimate sources. Money laundering is thus

always associated with an under-lying proceed-generating crime, the so-called predicate crime. Money laundering schemes can be very simple or highly sophisticated. Examples of simple money laundering operations are breaking up large amounts of cash into smaller sums and depositing into a bank account, transporting cash across borders, or buying high value goods such as artworks or precious metals and stones. A more sophisticated money laundering operation might involve a complex layer of financial transactions, such as converting cash into monetary instruments or using offshore shell companies to disguise the origin of the proceeds.

1.7 What is terrorist financing?

1.8 Terrorist financing is the process of directly or indirectly raising/collecting, moving, or using funds to support terrorist activities, individual terrorists, or terrorist organisations. These funds can be used for various purposes, including planning attacks, recruiting members, spreading propaganda, acquiring weapons, and establishing networks or safe havens. The funds used for terrorism can come from both legal and illegal sources, making it challenging to detect.

1.9 What are the main differences between money laundering and terrorist financing?

1.10 The Customer Due Diligence (CDD) requirements that so-called obliged entities, including exchange companies, have to comply with, are very much the same for money laundering and terrorist financing, since financial institutions and the other relevant businesses and professions (the so-called "Designated Non-Financial Businesses and Professions" or simply "DNFBPs") can be misused by both money launderers and terrorist financiers. However, conceptually there are differences between the two types of serious crimes, some of which are shown in the table right below:

	Money Laundering	Terrorist Financing
Motivation	Financial gain and/or financing of new crimes.	Funding of terrorist activities, for example for political or ideological reasons.
Source of funds	Always an underlying predicate crime to generate the proceeds.	The funding can be through both legal and illegal sources.
Amounts involved	Often involves large sums of money.	Generally, smaller amounts are needed for the terrorist activities, so transactions are often smaller and thereby hard to detect.
Methods of concealment	Both simple and complex money laundering schemes exist, but professional money launderers often use complex transactions, shell companies, offshore accounts, and investments to make funds appear legitimate.	Often uses simpler and harder-to-detect methods, like small wire transfers, cash smuggling, crowdfunding, or "front" organisations such as charities.

2 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH EXCHANGE COMPANIES

2.1 The Financial Action Task Force (the FATF) is the most important global standard setter in relation to Anti-Money Laundering (AML) and Combatting the Financing of Terrorism (CFT). FATF Recommendations 22 and 23 oblige exchange companies to comply with AML/CFT obligations. FATF has also issued a 2009 report titled *"Money Laundering through Money Remittance and Currency Exchange Providers"* that concludes that money transfers and exchange are particularly vulnerable to placement and layering stages of money laundering and that conversion into foreign currencies for example can facilitate cross-border money laundering.

2.2 The money laundering and terrorist financing risks associated with exchange houses in Kuwait are addressed in the June 2022 money laundering and terrorist financing National Risk Assessment of Kuwait and in the AML/CFT Mutual Evaluation Report (MER) of Kuwait adopted October 2024 by the FATF.

2.3 The June 2022 National Risk Assessment of Kuwait

2.4 Kuwait in June 2022 adopted a National Risk Assessment (NRA) on money laundering and terrorist financing. The following is stated about the money laundering risk associated with exchange companies:

"Exchange companies in Kuwait are exposed to ML risks rated at Medium-High (MH) level, resulting from the Medium-High (MH) threat level the Sector is exposed to, and its Medium (M) level vulnerabilities"

"The above is because Exchange Companies Sector is a major crossing point in the field of external financial transfers and given the great importance of those companies in shaping the Financial Institutions Sector in Kuwait due to the nature of their activity, through which several customers are dealt with, in addition to the volume of implemented financial transactions. Therefore, Exchange Companies Sector are one of the sectors targeted for exploitation in the field of money laundering operations"

2.5 The October 2024 Mutual Evaluation Report (MER) of Kuwait

2.6 It is mentioned in the MER that the ML risks in the financial sector are the highest in relation to banking, exchange companies and securities (MER p. 15). At p. 23 of the MER the assessors ranked the sectors based on their relative importance in Kuwait's context given their respective materiality and level of ML/TF risks. The following is of particular relevance to this Guidance Note:

"The exchange company sector is also weighted heavily based on materiality and risk. There are 32 exchange companies in Kuwait that administer remittances to numerous countries in order to meet the needs of the large number of foreign workers in Kuwait."

3 HIGH-LEVEL AML/CFT CUSTOMER DUE DILIGENCE (CDD) REQUIREMENTS FOR EXCHANGE COMPANIES OF RELEVANCE TO THE REPORTING OBLIGATION

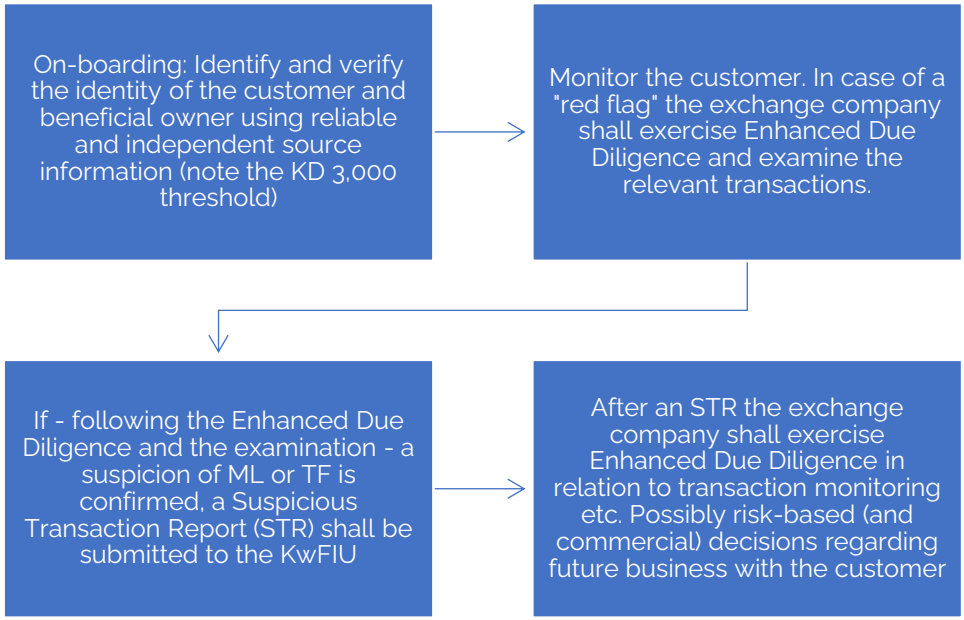
3.1 Relevant legal basis

3.2 International organisations such as the FATF have defined standards on how countries are supposed to fight money laundering and terrorist financing. There are several different provisions, many of them of relevance to the reporting obligation. Kuwait have implemented these standards into national policies, co-operation practices between the relevant authorities, and legislation. In relation to exchange companies in Kuwait the following legal acts are particularly relevant:

- Law no. 106 of 2013: This is the general AML/CFT Law that applies to all financial institutions and DNFBPs, including exchange companies.
- Ministerial Resolution no. 37 of 2013 - Executive Regulation for Law 106 of 2013: Supports law no. 106 of 2013.
- Circular no. 2/ES/507/2023 concerning AML/CFT (CBK Instruction AML/CFT to exchange companies), dated 16/2/2023 .

3.3 High-level CDD requirements for exchange companies of direct relevance to the reporting obligation

3.4 The high-level AML/CFT Customer Due Diligence (CDD) requirements for exchange companies of direct relevance to the reporting obligation can be illustrated by the following process diagram:



3.5 According to article 1 of law 106 of 2013, a "customer" is any person for whom a transaction, business relationship or account is arranged, opened, or undertaken. A customer is also any signatory, any person to whom an account, rights or obligations have been assigned or transferred, and any person who has authorised, controlled or initiated a transaction, a business relationship or an account.

3.6 According to article 1 of law no. 106 of 2013, a "business relationship" is expected to have an element of duration. As for exchange companies, stand-alone exchange operations probably does not live up to being a "business relationship".

3.7 Article 6 of the Ministerial Resolution no. 37 of 2013 makes a reference to article 5 and defines "the applicable threshold" to be KD 3,000 (or equivalent). This would seem to suggest that the obligation to identify and verify the identity of a customer or beneficial owner only applies when the transaction, business relationship or account is at least KD 3,000.

3.8 Article 16 of the Ministerial Resolution defines a time limit of 2 days for reporting to the KwFIU after a suspicion (or reasonable grounds to suspect) has materialised.

3.9 "Red flags" specifically for exchange companies will be detailed below under section 4 of this Guidance Note and the reporting obligation, including the concepts of an STR and an FIU, will be detailed further under section 5.

4 RED FLAGS FOR MONEY LAUNDERING OR TERRORIST FINANCING IN THE EXCHANGE COMPANIES SECTOR

4.1 As mentioned above in the process diagram a so-called "red flag" requires the exchange company to conduct Enhanced Due Diligence and examine the transaction in question. A "red flag" is a warning sign or indicator that suggests a transaction, activity, or behavior may be suspicious and could be linked to money laundering, terrorist financing, fraud, or other financial crimes. Red flags do not automatically mean that a crime has been committed, but they signal the need for further diligence and examination.

4.2 Key characteristics of a red flag are mentioned in article 5 of law 106 of 2013:

(i) Complex unusual large transactions

(ii) Unusual patterns of transactions for which there are no clear economic or visible lawful purposes or objectives

4.3 The transactions in question can be transactions deviating from normal business or customer behaviour, or transactions not matching the customer's known profile, financial history or industry standards, or transactions to which the customer cannot provide a clear or logical explanation, or transactions involving high-risk jurisdictions.

4.4 A red flag will depend on the sector or profession in question. Even within a specific sector or profession (in this case exchange companies in Kuwait) the red flags will depend on the legislative, financial, commercial and product framework.

4.5 For exchange companies in Kuwait the following types of money laundering and terrorist financing red flags can be relevant, again depending on the activities conducted by the individual exchange company:

(i) Customer profile and behaviour

(ii) Transaction patterns and characteristics

(iii) Use of proxies and third parties

(iv) Currency exchange specific red flags

(v) Money transfer specific red flags

(vi) Terrorist financing specific red flags

4.6 **Customer profile and behaviour**

4.7 Unusual or inconsistent identification and disclosures

- Customer provides incomplete, false, forged, or inconsistent personal identification or address documents
- Customer refuses to disclose or provides vague answers about the source of funds or economic activity

4.8 Suspicious conduct

- Customer appears overly anxious, secretive, or defensive when asked basic due diligence questions
- Customer is overly familiar with AML/CFT procedures or thresholds and attempts to dictate how transactions should be recorded.

4.9 **Transaction patterns and characteristics**

4.10 Structuring and avoidance of thresholds

- Customer breaks large transactions into smaller ones just under the reporting or verification limits over short periods
- Use of multiple individuals (possibly "smurfs") to send or exchange amounts just below thresholds on the same day or within a short span.

4.11 Unusual frequency, volume, or transaction size

- Repeated high-value transactions inconsistent with customer's declared income, occupation, or expected activity

- Sudden increases in the size or frequency of transactions without a plausible explanation or business rationale

4.12 Unusual payment routing or destination

- Frequent transactions to or from high-risk jurisdictions, conflict zones, or countries with known terrorist presence
- Use of multiple locations or agents to send/receive transactions that could reasonably be completed from a single point.

4.13 Jurisdictional and geographic red flags

- Transactions involving countries or regions subject to sanctions, embargoes, or with weak AML/CFT controls as identified by the FATF or local authorities
- Customer frequently receives funds from or sends funds to offshore financial centers, tax havens, or jurisdictions known for banking secrecy
- Customer has no apparent ties to a jurisdiction yet conducts significant financial activity involving that region (e.g., no business, family, or travel links)
- Transactions involve routing through multiple intermediary countries for no clear commercial or logistical reason

4.14 **Use of proxies and third parties**

4.15 Transactions on behalf of others

- Customer conducts transactions for third parties without a clear legal relationship (e.g., unrelated persons sending money for each other)
- Frequent use of the same individual to send/receive funds for multiple, unrelated customers.

4.16 Multiple senders or beneficiaries

- Several individuals sending remittances to a single beneficiary or one individual sending to multiple recipients without apparent family or business ties
- Beneficiaries or senders are frequently changed or rotated without clear explanation.

4.17 **Currency exchange specific red flags**

4.18 Large or repetitive cash exchanges

- Customer frequently exchanges unusually large amounts of cash in local or foreign currency without providing a plausible purpose (e.g., no travel plans, no business context, no investment rationale)
- Pattern of multiple same-day or consecutive-day visits to exchange similar amounts of cash that together exceed thresholds, suggesting structuring to avoid reporting
- Regular exchange of high-value currencies such as USD, EUR, or GBP without a declared reason or record of travel, business activity, or family obligations abroad

4.19 Unexplained currency movements or conversion patterns

- Customer conducts "round-trip" currency exchanges (e.g., converting large sums to foreign currency and then back to local currency within days) with no clear economic purpose, possibly to obscure source of funds or simulate legitimate activity

- Customer frequently requests foreign currency that is not commonly used for travel or commerce from Kuwait (e.g., unusual interest in currencies of conflict-affected or sanctioned jurisdictions)
- Transactions involving repeated conversion of small denominations to large ones (or vice versa) without any apparent business or personal reason

4.20 **Money transfer specific red flags**

4.21 Transfers inconsistent with customer's declared profile

- The value or volume of funds being remitted far exceeds the customer's stated occupation or declared income (e.g., domestic worker or low-income laborer sending large monthly remittances)
- Infrequent or dormant customers suddenly initiating high-value or frequent transfers to multiple recipients, especially abroad, without change in profile or declared purpose
- A customer sends or receives remittances under business pretense (e.g., "trade settlement") but provides no company registration, invoices, or contracts to support the claim.

4.22 Attempts to conceal identity or transaction purpose

- Customer avoids providing beneficiary details or shows discomfort when asked about the relationship or purpose of transfer, often responding with vague or generic reasons such as "personal" or "family."
- Use of inconsistent, incorrect, or unverifiable sender or recipient names — or provision of documents that appear forged, expired, or borrowed from others.
- Frequent changes in sender or recipient names with identical transaction characteristics, suggesting attempts to mask flow of funds through aliases or strawmen
- Use of remittance services to send funds on behalf of third parties who are not present, often claiming to be "helping a friend" or "asked by someone," with no documentation or clear legal basis.

4.23 **Terrorist financing specific red flags**

4.24 Transactions linked to conflict zones or high-risk areas

- Frequent or large transactions to jurisdictions associated with terrorism financing or designated conflict zones
- Transfers to border areas or regions with limited financial infrastructure, especially where terrorist groups are active

4.25 Suspicious use of charities or informal networks

- Transactions referencing NPOs, charities, or religious organisations with unclear or unverifiable legitimacy
- Individual repeatedly collects or distributes funds claiming charitable or humanitarian purposes with no transparency or reporting

4.26 Small, repetitive transfers indicative of operational funding

- Numerous low-value transfers that appear structured or sent from/to multiple individuals within a network

- Sender or recipient involved in what appears to be funding logistical support (e.g., travel, lodging) without a clear commercial or personal link

4.27 Customer profile matches terrorism risk indicators

- Customer is known to law enforcement or security agencies as linked to radicalism or terrorism, or is a close associate of such individuals (and this information is publicly available)
- Customer has a travel history to or from conflict zones without reasonable explanation (e.g., Syria, Iraq, Afghanistan) (and this information is publicly available)

5 EXAMINATION AND REPORTING OF SUSPICIOUS TRANSACTIONS

5.1 As mentioned above under section 3, it follows from article 5 of law no. 106 of 2013, that a transaction needs to be further examined if it is complex and unusually large or if there is a pattern of transactions for which there are no clear economic or visible lawful purpose or objective. The red flags are used to determine whether such an examination is needed.

5.2 An examination according to article 5 is usually conducted by the risk function of the business entity or the compliance function, i.e., operational staff with insights into money laundering and terrorist financing risks. If this function assesses the transaction to be suspicious this assessment is usually escalated up the formal hierarchy in the exchange company and the formal decision to submit a report to KwFIU is usually taken by persons higher up the formal hierarchy. In some reporting entities, there is a designated committee established for this purpose, however, due to their usual size this is probably not the case with exchange companies,, where the decision normally would be taken by the Director or owner.

5.3 The legislation does not define a maximum timeline for the examination, just like there is no timeline defined for the escalation and formal decision-making by the hierarchy of the exchange company. However, these processes obviously need to be concluded as quickly as possible.

5.4 Suspicious transaction reporting

5.5 When the exchange company has taken the formal decision that a transaction shall be deemed suspicious, a Suspicious Transaction Report (an "STR") shall be sent to the KwFIU, which is the national Financial Intelligence Unit ("FIU") of Kuwait. Exchange companies shall report *"without delay"* suspicious transactions or attempted transactions.

5.6 The term *"without delay"* gives very little time available, and in any case the STR needs to be submitted to KwFIU no later than 2 working days after the suspicion (or reasonable grounds to suspect) has materialised (se article 16 of the Ministerial Resolution no. 37 of 2013).

5.7 It follows explicitly from both article 12 of law no. 106 of 2013 and article 15 of Ministerial Resolution no. 37 of 2013, that a suspicion has to be reported *"regardless of its value"*. In that context the threshold of KD 3,000 that follows from article 6 of the Ministerial Resolution should be born in mind, meaning that in reality an STR might be required even where the exchange company has not (yet) exercised CDD against the customer.

5.8 An STR is not a police complaint or a police report, and the STR cannot be used by law enforcement or prosecution as evidence of criminality. An STR is a piece of intelligence that the KwFIU can use in its' work.

5.9 An STR shall usually detail the following:

(i) The customer in question, i.e., name, address, ID, occupation etc.

(ii) The transaction in question, i.e., amount, currency, date, method, involved parties, purpose etc.

(iii) All information related to the examination leading to the reporting, including analysis

(iv) The reason for suspicion, i.e., explanation of the "red flags" (this part of the STR is called the narrative).

(v) Supporting documentation (if applicable), e.g. transaction transscripts, copies of CDD documents etc.

5.10 It is important to note, that it is illegal to inform a customer about an STR being submitted to the KwFIU (so-called tipping off).

5.11 **Role of the KwFIU**

5.12 The legal basis for the KwFIU is article 16 of law 106 of 2013, whereafter a unit called the "Kuwait Financial Intelligence Unit" shall be established. The KwFIU is an independent legal person and serve as the agency responsible for receiving, requesting, analysing, and disseminating information concerning suspected proceeds of crime or funds related, linked to or to be used for money laundering or terrorism financing. The KwFIU is not a law enforcement body but an administrative authority.

5.13 STRs submitted to KwFIU need to be communicated via a digital platform called GoAML, that all reporting entities in Kuwait are obliged to use.

5.14 The KwFIU conducts strategic analysis of important topics related to money laundering and terrorist financing. The KwFIU also conducts operational analysis of the STRs received from exchange companies and other professions comprised by law 106 of 2013, not least the financial sector. When the operational analysis made by the KwFIU confirms the suspicion of money laundering or terrorist financing, it follows from law no. 106 of 2013 that a dissemination report has to be sent to the Public Prosecutor's Office (PPO). Often the PPO would then decide that the Money Laundering Unit or the Terrorist Financing Unit of the Ministry of Interior (MOI) should carry out the preliminary investigation, including collection of evidence, whereafter the PPO will decide whether to prosecute or not.

5.15 The KwFIU is also responsible for identifying high-risk countries and prescribe the measures to be applied in relation to such countries.

5.16 The KwFIU is authorised to obtain from any person subject to the reporting obligation in law no. 106 of 2013 any additional information it deems necessary to carry out its functions.

---oooOooo---