GUIDANCE NOTE

REPORTING OBLIGATIONS FOR BANKS 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. Banks and other financial institutions play an important role in protecting Kuwait against these kinds of crimes.

1.2 **Banks covered by the legislation on money laundering and terrorist financing**

1.3 Banks are covered by law no. 106 of 2013 on Anti-Money Laundering and Combatting the Financing of Terrorism.

1.4 Article 1 of law no. 106 of 2013 defines the concept of a "financial institution" as:

"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:"

1.5 Article 1 of law no. 106 of 2013 then goes on by listing all the different activities or operations, that qualify as a "financial institution" when conducted as a business. These include acceptance of deposits and other repayable funds from the public, including private banking, lending, financial leasing, money or value transfer services, financial guarantees and commitments, foreign exchange transactions, and many others.

1.6 **What is money laundering?**

1.7 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.

1.8 **What is terrorist financing?**

1.9 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.

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

1.11 The Customer Due Diligence (CDD) requirements that so-called obliged entities, including banks, have to comply with, are very much the same for money laundering and terrorist financing, since the financial system and the other relevant businesses and professions (the so-called "Designated Non-Financial Businesses and Professions" or simply "DNFBPs") can be misued 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 THE BANKING SECTOR

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). With banks being an essential financial vehicle it is natural that FATF in several policy documents has addressed the money laundering and terrorist financing risks associated with banking activities. For example there is a 2014 *"Guidance for a Risk-Based Approach - The Banking Sector"* and both the 40 Recommendations and the Interpretative Notes have many references to banks, including correspondent banking relationships and shell banks.

2.2 The money laundering and terrorist financing risks of the banking sector specifically for 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 banking sector and the money laundering risk:

"Banking Sector is among the sectors that have a significant and effective impact on economic activity in Kuwait. It consists of a group of local banks and branches of foreign banks subject to the supervision of the Central Bank of Kuwait."

"Kuwait Banking Sector is exposed to ML risks at Medium (M) level, due to the determined High (H) level threats, and vulnerabilities determined at Medium-Low (ML)"

2.5 As for the terrorist financing risk of the banking sector the following is noted in the NRA:

"The aforementioned sector [the banking sector] is used in terrorist financing crimes, due to the development of banking services in transferring funds through electronic applications and text messages that carry an electronic link for payment via smart devices. Further, most of the defendants withdraw money to be sent to terrorist organizations from their bank accounts and present them (in cash) to the organizers who deliver those funds. However, it should be noted that the level of targeting is low (L) due to the role and efforts of the regulatory authorities in the State of Kuwait in deterring crime, which explains the continued low level of terrorist financing cases in the country."

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

2.7 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. Specifically in relation to banks, they are responsible for well over half of the suspicious transaction reports submitted to KwFIU. In the MER there is no specific mentioning of the TF risk associated with the banking sector.

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

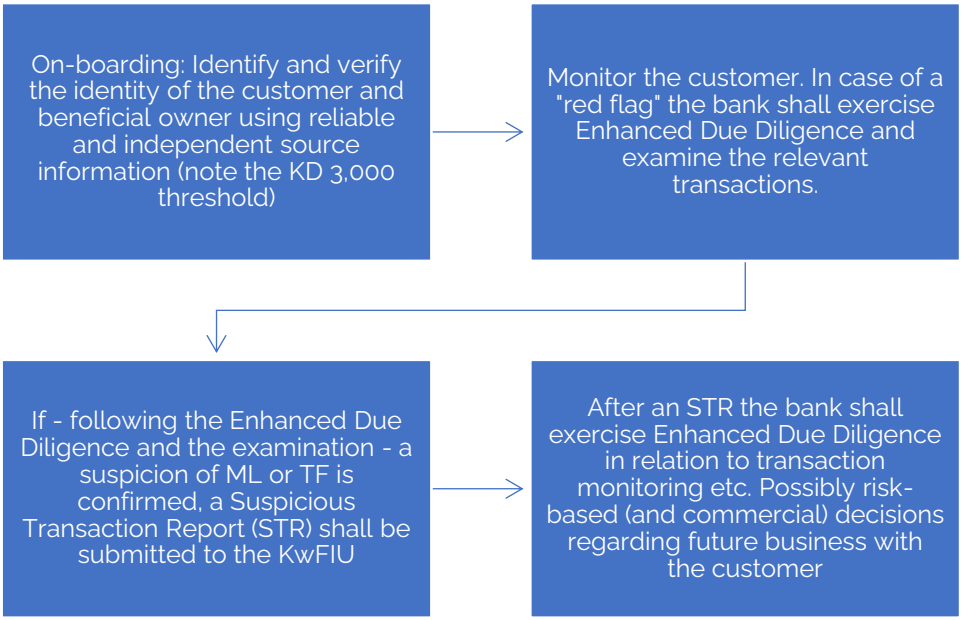
3.1 Relevant legal basis

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 banks 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.
- Ministerial Resolution no. 37 of 2013 - Executive Regulation for Law 106 of 2013: Supports law no. 106 of 2013.
- Circular (2/BS/IBS/507/2023) containing an an Instruction from the Central Bank of Kuwait (CBK) to banks concerning AML/CFT, dated 16/2/2023.

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

3.4 The high-level AML/CFT Customer Due Diligence (CDD) requirements for banks 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.

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 banks 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 BANKING SECTOR

4.1 As mentioned above in the process diagram a so-called "red flag" requires the bank 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 banks in Kuwait) the red flags will depend on the legislative, financial, commercial and product framework.

4.5 For banks 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 bank:

(i) Customer risk profile

(ii) Transaction and account activity risks

(iii) Product/service misuse

(iv) Jurisdictional risks indicators

(v) Structural and ownership risks

(vi) Suspicions linked to fraud

(vii) Alerts and adverse media

(viii) Terrorist financing specific red flags

4.6 **Customer risk profile**

4.7 Identification and Due Diligence

- Unclear or falsified identification documents
- Reluctance to disclose beneficial ownership or source of wealth/source of funds
- Discrepancies between declared and observed economic activities

4.8 Politically Exposed Persons (PEPs)

- Wealth or assets/incoming funds not justified by position or salary
- Involvement of family members or close associates in financial activity
- Use of complex structures to conceal involvement of a PEP

4.9 Unusual Customer Behavior

- Avoids face-to-face contact or insists on secrecy
- Displays evasiveness or overreaction to KYC inquiries
- Constant changes to address, contact information, or account signatories

4.10 **Transaction and account activity risks**

4.11 Cash and Payment Flows

- Structured cash deposits or withdrawals (smurfing)

- Sudden high-volume transactions without clear rationale
- Third-party deposits or payments inconsistent with account profile

4.12 Lending and financial guarantees

- Loans repaid early in lump sums from opaque sources
- Guarantees issued for unfamiliar counterparties or without sound business logic
- Requests for letters of credit or guarantees linked to shell companies

4.13 Account Usage Patterns

- Inactivity followed by bursts of high-volume transactions
- Incoming funds quickly sent offshore with no business justification
- Personal accounts used for apparent commercial activity or vice versa.

4.14 **Product/service misuse**

4.15 Trade finance and letters of credit

- Mismatches in documentation: inconsistent invoices, over/under-invoicing
- Re-export schemes without added value or economic logic
- Use of transit trade through high-risk jurisdictions

4.16 Correspondent Banking

- Respondent institutions with weak AML controls or operating in high-risk regions
- Pass-through transactions with no connection to underlying customer activity
- Unusual nesting of accounts with little visibility into underlying clients

4.17 Fund management and portfolio services

- Managing funds on behalf of multiple unrelated third parties
- Funds managed or invested from high-risk or sanctioned jurisdictions
- Sudden inflows/withdrawals from portfolios inconsistent with risk tolerance or investment profile

4.18 **Jurisdictional risk indicators**

4.19 High-risk jurisdiction exposure

- Transactions with or routed through jurisdictions listed by FATF (grey/black list) or under UN sanctions

4.20 Conflict or terrorism-linked regions

- Fund flows to/from countries known for civil unrest, conflict, or extremist presence
- Patterns of remittances to diaspora communities in terrorism-affected areas without economic linkage

4.21 Offshore and tax haven structures

- Use of shell companies or trusts incorporated in tax havens

- Customer maintains bank accounts or businesses in secrecy havens or listed jurisdictions
- Unexplained routing of funds through multiple offshore financial centers

4.22 **Structural and ownership risks**

4.23 Lack of legal and ownership transparency

- Complex structures masking ultimate beneficial ownership
- Frequent changes in ownership or unclear control chains
- Presence of nominee directors or signatories unrelated to business

4.24 Shell and front companies

- Entities with no real operations or physical presence
- Registered address shared with multiple unrelated entities
- Inflows and outflows with no explanation or links to stated business activity

4.25 **Suspicion linked to fraud**

4.26 Transactional behaviour suggestive of fraud

- Pattern of receiving large deposits followed by immediate withdrawals without clear economic justification
- Frequent transactions reversed shortly after being processed, especially where linked to disputed charges or suspected card fraud
- Sudden increase in transaction volume or value in accounts previously used for minimal activity, especially after online logins from new geographic regions
- Accounts receiving multiple small payments from different senders with similar references or patterns, commonly linked to fraud aggregation techniques (e.g., coordinated scams or money flipping)

4.27 Customer profile and link to known schemes

- Customer or account linked to known fraud schemes such as phishing, business email compromise, or investment scams
- Transactions associated with known mule accounts or money mules recruited through online scams

4.28 **Alerts and adverse media**

4.29 External risk signals

- FIU alerts, international watchlists, or public domain reporting (e.g., sanctions, criminal cases)
- Customer, directors or beneficial owners named in foreign court proceedings or investigations

4.30 Internal system alerts

- Transaction monitoring systems flag repeated rule breaches (e.g., velocity, volume, destination).

4.31 **Terrorist financing specific red flags**

4.32 Individual or entity-based risk

- Customer appears on national or international sanctions/watch lists
- Links to charities, trusts, or foundations with unclear source of funding or beneficiaries
- Use of personal accounts to receive or distribute pooled funds

4.33 Transaction patterns indicating TF

- Frequent low-value transfers to known conflict zones
- Funding donations or community collections without transparency
- Funds being sent to abroad and then shortly thereafter returned without economic reason
- Transactions involving significant amounts of cash, in particular withdrawals close to border points

4.34 Non-Profit Organisation risk

- NGO accounts sending large volumes abroad without programmatic expenses locally
- Donations structured to avoid detection (e.g., under thresholds)
- Use of hawala or informal MVTS systems outside of regulation.

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 bank and the formal decision to submit a report to KwFIU is usually taken by persons higher up the formal hierarchy.

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 bank. However, these processes obviously need to be concluded as quickly as possible.

5.4 Suspicious transaction reporting

5.5 When the bank 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. Banks 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 bank 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 nar,rative).

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

(vi) related to many transactions , it should mention dates of Suspicious period .

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 banks 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---