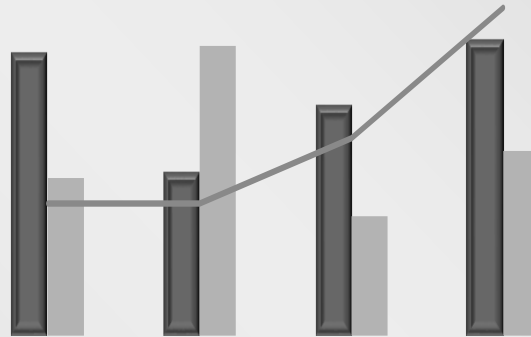




Anti-Money Laundering & Counter Terrorist Financing Unit

## Strategic Analysis



Trends, patterns and indicators of money laundering and terrorist financing in the Hashemite Kingdom of Jordan based on the database of the Anti-Money Laundering and Counter Terrorist Financing Unit

The Hashemite Kingdom of Jordan

Anti- Money Laundering & Counter Terrorist Financing Unit

٢٠٢٠

## Index

Introduction:	1
First: Work Mechanism and Methodology	2
Second: ML and TF Risks, and the Current Issues	3
Third: Analysis of quantitative and qualitative data and information	5
• Classification of notifications and reports according to the sending entity	5
• Classification of notifications and reports according to the suspicion:	9
• Classification of notifications and reports according to the type of financial instruments and methods used by the suspect/s:	12
• Cooperation requests with counterpart units:	14
Forth: Trends	15
Fifth: Patterns and practical cases	16
• First pattern: Smuggling of gold and precious metals through the passengers airport	16
• Second pattern: tax evasion by using the personal account for commercial purposes	19
• Third pattern: impersonation of princes from the Gulf countries to delude people for collecting donations to help the poor through social media channels	20
• Forth Pattern (terrorist financing): Collecting cash donations through social media channels without obtaining an official authorization:	22
Sixth: indicators	23
• ML indicators	23
• Terrorist financing indicators:	25
Seventh: Recommendations	26

### Introduction:

Money laundering and terrorist financing constitute two financial offences that result in significant economic implications, in addition to being a direct threat to the financial sector of the affected country and its stability in general. Effective anti-money laundering and counter terrorist financing systems are considered necessary to protect the integrity of markets and soundness of the global financial sector, as they help to mitigate factors, which facilitate financial exploitation. Therefore, taking necessary measures to prevent and combat money laundering and terrorist financing helps countries protect their financial and economic systems. Since the Hashemite Kingdom of Jordan is not immune to these two offences, being an effective part of the global economic system, officials in the Kingdom have drawn attention to the seriousness of these offences and the need to combat them and reduce their risks.

The strategic analysis outcomes help the Financial Intelligence Unit (FIU) and other relevant supervisory, security, regulatory, and administrative authorities understand the different and new patterns and trends of money laundering and terrorist financing.

The strategic analysis also helps to identify the surrounding and internal risks of the country, which, therefore, helps in setting priorities to face these risks and determine the mechanism for reducing them.

The development of knowledge at the FIU is one of the most important findings of the strategic analysis process, as knowledge is one of the first steps through which the security of the country's financial system is protected from the threats it faces.

## First: Work Mechanism and Methodology

- **Time Frame:**

The time period during which the notifications and reports received by the Unit were examined extends from 2016 until the end of 2019.

- **Objectives:**

Identifying the trends, patterns, and indicators of money laundering and terrorist financing operations in the Kingdom.

- **Scope:**

The information obtained and collected to prepare this report were received from the following sources:

- The Unit's database, which contains information on the notifications and reports received from the entities subject to the law and the entities reporting in accordance with the law.
- Relevant information obtained from counterpart Units under information exchange requests and automatic information requests.
- Any other relevant information from official government sources, including related judicial decisions.

- **Methodology**

- Distributing and identifying tasks to analysts in the Financial Investigation and Analysis Directorate.
- Studying cases available on the Unit's database in order to divide them according to the patterns and methods on which they are based, and to extract suspicion indicators.
- Reviewing and studying requests for information issued from and received to the Unit, especially those related to the cases available on the Unit's database, and requesting any additional information if needed.
- Conducting a study of the information collected through the graphs.

### **Outcomes:**

- Identifying trends, patterns, and indicators of money laundering and terrorist financing operations.
- Identifying weaknesses in order to develop a plan for addressing them.
- Coming up with appropriate recommendations for the outcomes reached.

## Second: ML and TF Risks, and the Current Issues

1. Findings of the national assessment of money laundering risks show that the overall risks level of money laundering in the Kingdom is "high", and the level of money laundering threats resulting from domestic proceeds of predicate offences in the Kingdom is "medium", constituting 93% of the total proceeds of domestic offences including tax evasion, "robbery (criminal theft) and theft", trafficking in narcotic drugs and psychotropic substances, and "corruption and bribery."

The assessment findings also show that most of the domestic proceeds of the predicate offences were generated in the form of cash; a significant part of which was spent through the use of the informal sector, and another part of these funds, especially those obtained through tax evasion, was laundered through the use of the financial sector. Moreover, it is found that there is a small percentage (approximately 18%) of the volume of domestic proceeds of predicate offences has been removed from the Kingdom. The money-laundering threat resulting from proceeds of international predicate offences was relatively small and assessed as being at a "low" level.

The findings also indicate that the banking sector, financial service providers including (money exchange companies, and payment and electronic transfer service providers), and the designated non-financial businesses and professions (DNFBP) are the highest at the level of net money laundering risks (after considering the impact of controls). Banks got a "high" level of risks, whereas the financial service providers and the DNFBP sectors obtained a "medium" level. Furthermore, results also show that financial brokerage companies, other financial companies, and non-profit organizations were the lowest at the level of net money laundering risks.

2. As for terrorist financing, findings of the national assessment of terrorist financing risks show that the overall level of risks of terrorist financing in the Kingdom is "medium", and that the result of assessing the level of terrorist financing threats resulting from local fundraising is "medium". It is also found that the funds collected to be used in terrorist acts are obtained mainly from voluntary donors (self-financing from those in charge of the terrorist act, or sympathizers or supporters of their ideas), or from donors against their will or who do not know the destination of the money. Besides, it has been revealed that there are no organized groups in the Kingdom known to collect money for terrorists, bearing in mind that the money collected was mainly in the form of cash, half of which remained inside the kingdom and the other half was sent abroad to be used by foreign terrorist fighters or for the purposes of financing them. The number of Jordanian fighters existing in extremist organizations outside Jordan reached (1325). It was found that the terrorist financing threats resulting from cash flows into the Kingdom are relatively small, and assessed as being at a "low" level, and that more than (90%) of the financing operations are conducted through the informal financial sector.

In addition, results reveal that the banking sector and the financial services providers' sector (including money exchange companies, and payment and electronic transfer service providers) are the highest at the level of net terrorist financing risks due to having a "medium" level, followed by the DNFBP and the insurance sectors with a "low" level of risk.

3. It is also indicated that there are some current issues in the Kingdom, namely:
- The occurrence of some terrorist operations inside the Kingdom over recent years, which were adopted by agents being sympathetic to terrorist organizations.
  - The aggravation of turmoil and the state of chaos still faced by some countries in the region, especially those surrounding the Kingdom and which suffer from security tensions.
  - The economic pressures facing the Kingdom, which may lead to an increase in crime rates.

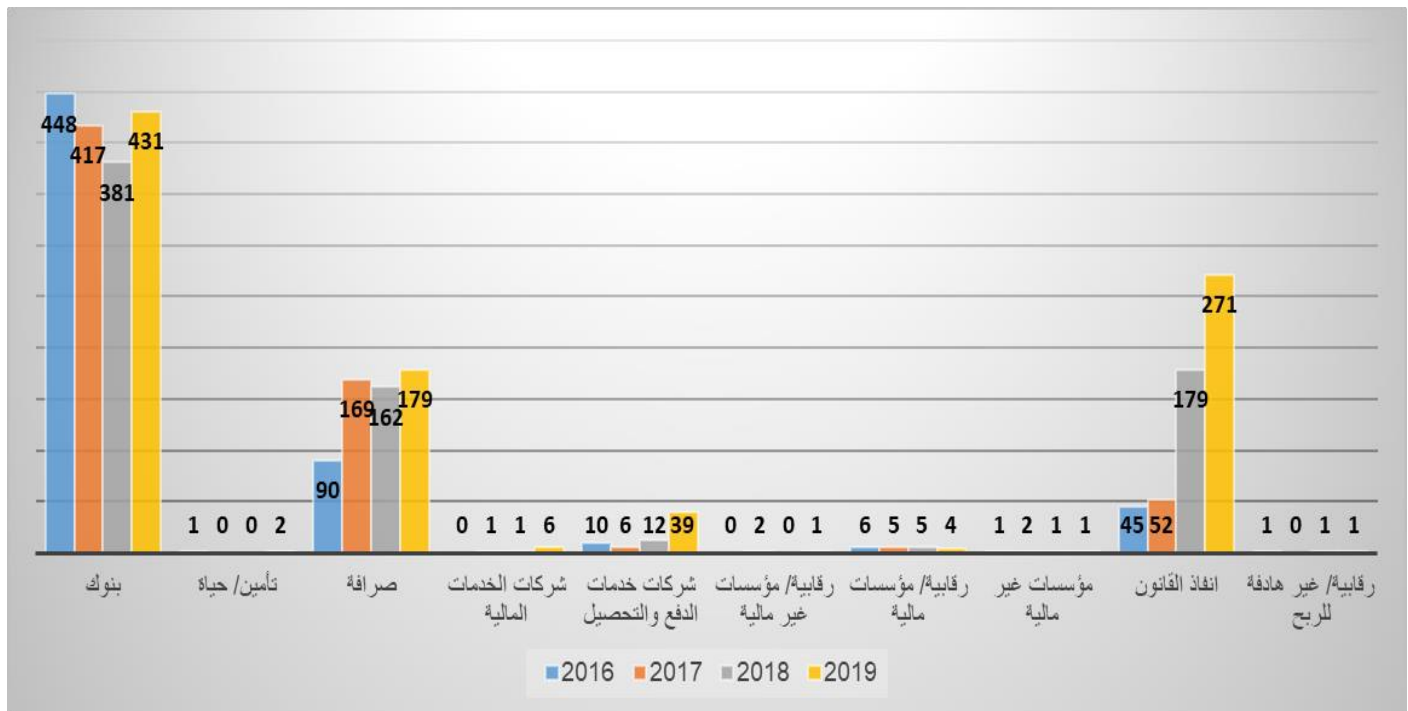
### Third: Analysis of quantitative and qualitative data and information

The Unit's database for the years (2016) until (2019) was examined. Notifications and reports received by the Unit were classified into three categories. In the first category, they were distributed according to the entity sending the notification and the report, whereas in the second category they were distributed according to the suspicion and type of suspected crime, and in the third category they were distributed according to the type of financial instruments used by the suspects.

Moreover, the notifications and reports were studied in terms of suspicion indicators contained therein and the quality of information provided by the reporting entities. Referrals and feedback from the entities to which the referral was made were also examined. The following are the most prominent results of the study: -

*Classification of notifications and suspicious reports according to the sending entity as follows:*

Entity	Number of notifications and reports			
	2016	2017	2018	2019
<b>Banks</b>	٤٤٨	٤١٧	٣٨١	٤٣١
<b>Money exchange firms</b>	٩٠	١٦٩	١٦٢	١٧٩
<b>Financial services companies</b>	٠	١	١	٦
<b>Insurance/ life Insurance</b>	١	٠	٠	٢
<b>Non-financial institutions</b>	١	٢	١	١
<b>Payment and collection services companies</b>	١٠	٦	١٢	٣٩
<b>Supervisory bodies over financial institutions</b>	٦	٥	٥	٤
<b>Supervisory bodies over non-financial institutions</b>	٠	٢	٠	١
<b>Supervisory bodies over non-profit organizations</b>	١	٠	١	١
<b>Law enforcement agencies</b>	٤٥	٥٢	١٧٩	٢٧١
<b>Total</b>	٦٠٢	٦٥٤	٧٤٢	٩٣٥



**After reviewing and analyzing the above table, the following has been concluded:**

- Banks continued to be the largest reporting entity for suspicious transactions during the study period (2016-2019), as the total number of notifications sent by them was (1677), representing (71%) of the total notifications received by the Unit, which indicates that banks are the most vulnerable to exploitation in money laundering operations. The reason for the high number of notifications received from banks is that they are fully aware that criminals tend to exploit this sector in money laundering and terrorist financing.
- It was noticed that the number of notifications received from licensed money exchange companies increased during the years from 2016 to 2019, as the percentage of the number of such notifications received from these companies during the year 2016 was (16.3%) of total notifications received in the same year, while it reached (27.2%) in 2019. Moreover, the number of notifications rose from (90) in (2016) to (179) in (2019); this is due to the increased awareness of compliance departments at money exchange companies as a result of the coordination meetings that the Unit holds with these entities, in addition to the adoption of systems for supervising and monitoring financial transactions by many of them.
- By studying the notifications received from money exchange companies operating in the Kingdom, it is found that they are related to suspicious remittances (issued and received) due to the nature of the services they are authorized to provide. This type of financial institutions is basically attractive to criminals since the transfer procedure does not require opening an account or giving detailed information to the money exchange company, in addition to the large number of money exchange companies which are (140 companies), the great number of their branches that are spread throughout the Kingdom, and the diversity and multiplicity of means and methods of financial transfers through money exchange companies.
- The existence of a trend to exploit banks and money exchange companies in money laundering and terrorist financing operations is consistent with the findings of the national risks assessment



in terms of risk classification of these sectors. It also emphasizes the need for these sectors to continue their strict supervision over the transactions conducted through them.

- There was a significant increase in the number of reports received from law enforcement authorities during the years 2018 and 2019 compared to 2016 and 2017. A total of (97) reports were received by the Unit during the years 2016 and 2017, while a total of (450) reports were received by the Unit during 2018 and 2019 with an increase of (364%). This indicates that law enforcement authorities are exerting more efforts in conducting parallel financial analyses and are relying more on the Unit to benefit from the financial information it has.
- It is also found that the notifications received from payment and collection services companies increased by (290%). After examining these notifications, it is noticed that most of them are related to suspicious transactions issued by credit cards belonging to persons of an Arab nationality. The most prominent indicators of suspicion in these cases are as follows:
  - a. The great and sudden change in the volume of transactions executed by dealers via the credit card payment service within a short period of time and without a clear economic justification.
  - b. A significant splitting of transactions without a clear economic justification, as a great number of transactions has been executed using a large number of such credit cards, taking into account that it is possible to make the payment through the card in one procedure without the need to split the transactions.
  - c. The nature of the dealers' activity is not commensurate with the volume of executed transactions, in addition to the difference in his/ her sales volume compared to his/ her counterparts of the same nature of activity within the same region.

After completing the Unit's investigation and financial analysis procedures, it is found that the source of funds in these cards is from the government of the country issuing them, and that they are being disbursed to its citizens to cover their living and medical treatment expenses. However, citizens take out these cards outside their countries with the aim of liquidating their value in cash and then returning these amounts to their country in cash to benefit from the currency difference, which is beneficial to them. This process is done in agreement with the dealers who make fake financial transactions via the electronic payment system using these cards, thus leading to the existence of huge financial transactions on the dealer's account with the service provider. Accordingly, the Unit has referred the issue of these notifications to three entities, namely: -

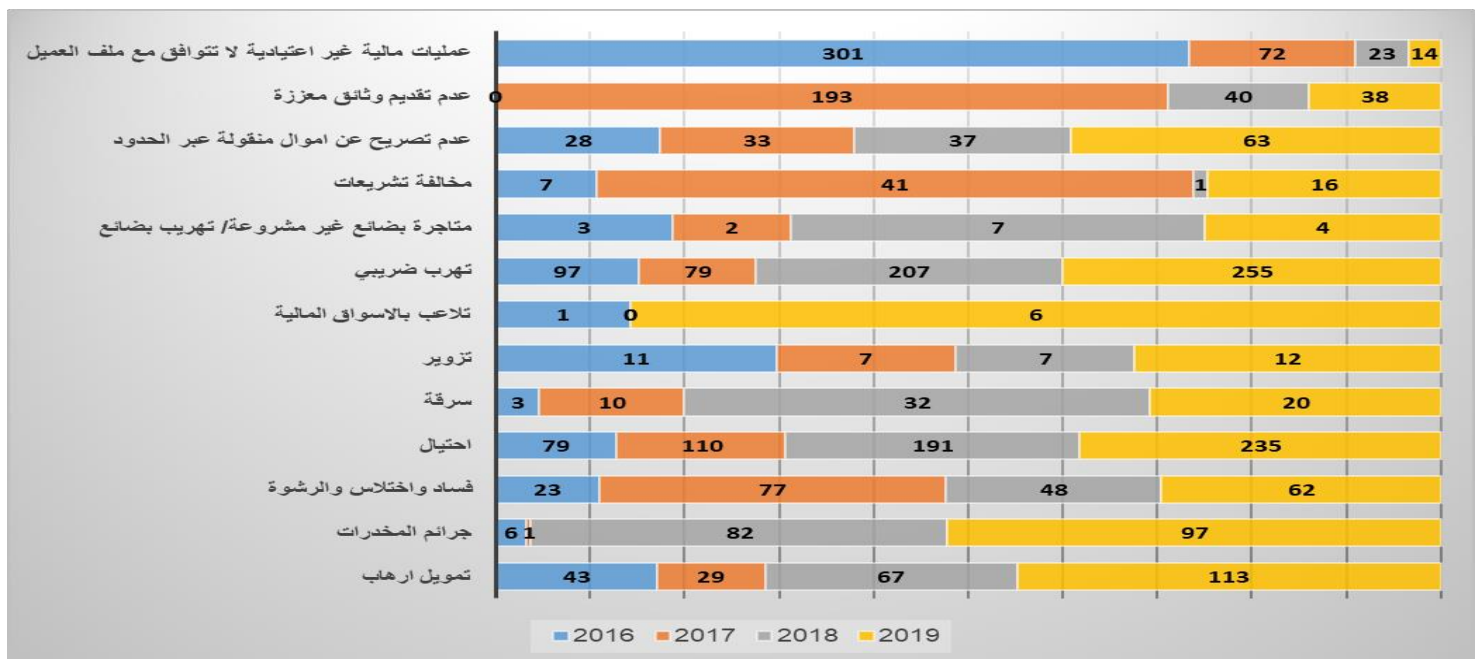
- ✓ The Financial Intelligence Unit of the country issuing the cards, as they were informed of the case and the results of the Unit's investigations, upon an outward automatic request for information.
- ✓ Competent security authorities: In order to introduce them to this new pattern that is carried out through money transfer transactions from Arab countries to Jordan using credit cards, then liquidating their value in cash and re-sending them to the country from which they were issued. Besides, since such activities has security risks, the referral has been made.
- ✓ Income and Sales Tax Department: Since the financial transactions carried out on the dealer' account were very large, and they were conducted through his business; therefore,

these transactions constitute a financial income, and due to the inability to verify whether the dealer pays income and sales tax on these transactions, the referral has been made.

The companies who reported these notifications were also addressed and informed of the results of investigation and analysis made by the Unit and the entity to which the referral has been made; they were also asked to provide the Unit with any developments they have regarding this issue.

*Classification of notifications and suspicious reports according to the suspicion:*

Type of instrument used	Number of notifications and reports			
	2016	2017	2018	2019
<b>Tax evasion</b>	97	79	207	200
<b>Theft</b>	3	10	32	20
<b>Drug offences/ Narcotics</b>	6	1	82	97
<b>Corruption, embezzlement and bribery</b>	23	77	48	62
<b>Fraud</b>	79	110	191	230
<b>Illicit trafficking in goods/ smuggling of goods</b>	3	2	7	4
<b>Manipulation of financial markets</b>	1	0	0	6
<b>Forgery</b>	11	7	7	12
<b>Non-declaration of funds transported across borders</b>	28	33	37	63
<b>Violation of regulations</b>	7	41	1	16
<b>Failure to submit supporting documents</b>	0	193	40	38
<b>Unusual financial transactions that are not consistent with the customer's profile</b>	301	72	23	14
<b>Terrorist financing</b>	43	29	67	113
<b>Total</b>	602	604	742	930



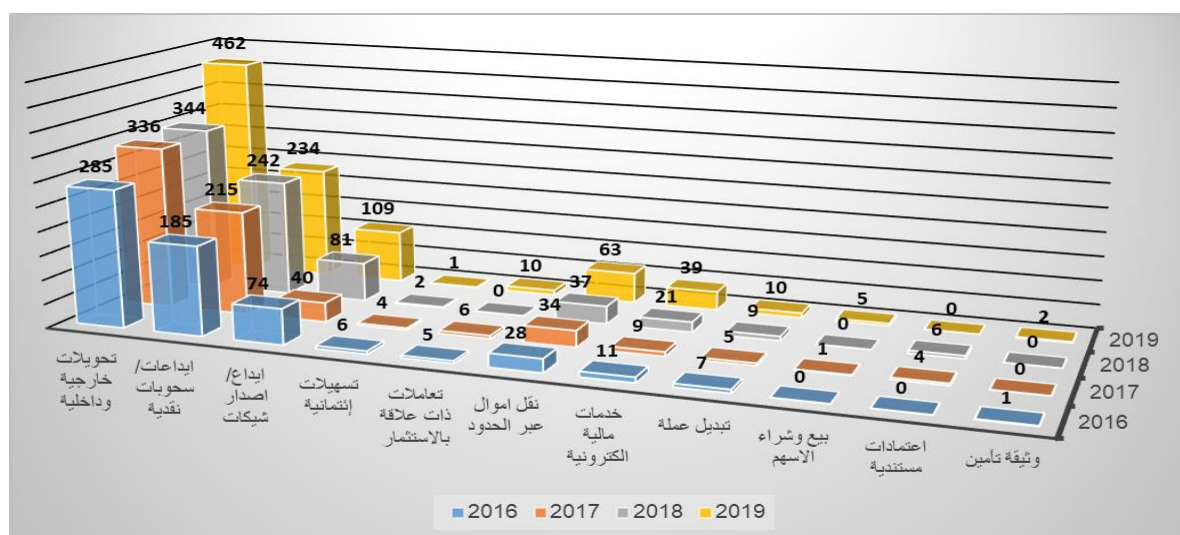
By examining and analyzing the figures shown in the table above, the following has been found:-

- It is indicated that there is an increase in the notifications and reports received by the Unit and related to suspected tax evasion as their number reached (97) in 2016, whereas they were (255) in 2019, with an increase of (162.8%).
- The number of notifications and reports received by the Unit on fraud increased during this period, being (79) during 2016, while they reached (191) and (235) in 2018 and 2019, respectively.
- The increase in the number of notifications and reports associated with tax evasion and fraud suspicions reflects the existence of a trend to launder money resulting from tax evasion and fraud through the financial sector. It also reflects the reporting entities' understanding of risks and their awareness that tax evasion and fraud offences are amongst the most common offences that generate proceeds, which is consistent with the findings of the national risks assessment. Furthermore, the increase confirms that such entities have adopted a risk-based approach and they strengthened their controls and procedures over any transaction suspected to have any connection with the tax evasion offence. This is due to the feedback that the Unit provides to the reporting entities regarding fraud patterns used by criminals in the financial sector.
- As for cross-border money transfers, an increase was noticed in the number of reports received from the Jordan Customs Department and related to the non-declaration or the false declaration over the study period, as (63) reports were received during 2019, while the Unit received only 28 reports during 2016.

- The increase in the number of reports received from the Jordan Customs regarding non-declaration and the false declaration is an indication of the efforts made by the Jordan Customs in the process of inspecting travelers coming to the Kingdom and reinforcing cooperation between the Unit and Customs, in addition to the awareness of the money laundering and terrorist financing risks outside the formal financial sector through the transfer of funds and cash across borders.
- The number of notifications and reports received by the Unit in 2017 and related to the reporting entity's suspicion that the customer did not provide the necessary supporting documents reached a total of (193), while this number decreased during 2018 and 2019 to (40) and (38), respectively. It is also revealed that there is a significant decline in the number of notifications and reports related to the suspicion of (unusual financial transactions) as the number was (301) during 2016, while it reached (14) during 2019. This indicates banks' compliance with the regulations issued by the Central Bank of Jordan in this regard, the development of their electronic systems and suspicion indicators, and the increased awareness among reporting entities of the need to better identify the causes and reasons for suspicion in order to improve the quality of notifications issued by them.
- As for cases suspected of terrorist financing, the following has been found:
  - a. The notifications received from the reporting entities significantly decreased throughout the study period, since the analyses showed that terrorists and terrorist financiers are using other means of financing through cash handling and fundraising (cash liquidity) or by self-financing (such as obtaining personal loans, selling their personal property for financing purposes, and using personal savings). This is confirmed by the findings of the national risks assessment which reveal that more than (90%) of financing operations are carried out through the informal financial sector.
  - b. There was also an increase in the number of reports received from law enforcement and judicial authorities regarding the terrorist financing suspicion and these authorities relied on the Unit in conducting the parallel financial analysis for these cases. Moreover, studies and analyses made by the Unit at the request of law enforcement and judicial authorities indicate an increase in the terrorist financing trend through the use of the informal sector and the possibility of the physical cross-borders transportation of funds (transportation of amounts less than the disclosure limit). This is followed by the need to strengthen security supervision at border crossings and on persons suspected of being involved or sympathizing with terrorists.

*Classification of notifications and suspicious reports according to the type of financial instruments and methods used by the suspect/s:*

Type of instrument used	Number of notifications and reports			
	2016	2017	2018	2019
Local and foreign transfers	٢٨٥	٣٣٦	٣٤٤	٤٦٢
Cash deposits/ withdrawals	١٨٥	٢١٥	٢٤٢	٢٣٤
Cheque deposit/ issuance	٧٤	٤٠	٨١	١٠٩
Credit facilities	٦	٤	٢	١
Investment transactions	٥	٦	---	١٠
Cross-border transportation of funds	٢٨	٣٤	٣٧	٦٣
Electronic financial services	١١	٩	٢١	٣٩
Currency change	٧	٥	٩	١٠
Sale and purchase of shares	---	١	---	٥
Insurance policy	١	---	---	٢
Letters of credit	---	٤	٦	٠



**By examining and analyzing the figures shown in the table above, the following has been indicated:**

- It is noted that the most common financial instruments being exploited by suspects in the notifications and reports received during the period from 2016 to 2019 are remittances, while the exploitation of cash deposits and withdrawals came in the second place, followed by the cheque deposit and issuance, which is placed third.
- After examining the notifications received by the Unit, it is revealed that there is a noticeable trend of using cash transfers, deposits, and withdrawals in tax evasion and fraud, which therefore explains that the most common financial instruments exploited by suspects are cash transfers, deposits and withdrawals. It is also found that the notifications associated with the fraud offence came mostly from money exchange companies; particularly those whose headquarters or branches are located in specific regions in the Kingdom. By reviewing these notifications, it became clear that most of them are related to the impersonation of public figures from Gulf countries in order to collect donations and financial aids for the Syrian community present in the Kingdom where donations are received through money transfers via money exchange companies, which in turn interprets the increased notifications received by the Unit from licensed money exchange companies.
- An increase was also noticed in the use of electronic financial services by suspects throughout the study period, as (39) notifications and reports related to the use of such instruments by suspects were received by the Unit during 2019, whereas there were (11) notifications and reports in 2016.
- The increase in suspected cases reported to the Unit and related to electronic financial services is an indication of the extent to which suspects and criminals have developed knowledge of modern technologies and how they can use it to carry out their criminal activities. Moreover, the use of e-wallets for money transfer purposes is considered a simple and uncomplicated process, and that the amounts of remittances transferred by these persons are small; therefore, encouraging them to use these methods.
- It is also indicated that there were few notifications and reports received by the Unit and related to financial instruments such as insurance policies, letters of credit, stock trading, currency exchange, and credit facilities, which therefore denotes the reluctance of criminals to use these instruments due to the difficulty of exploiting them in money laundering as well as the existence of strict supervision over their use.

*Cooperation requests with counterpart units:*

**1. Outgoing international cooperation requests of information:**

- (16) information requests were sent during 2016. It was noticed that the countries to which the requests were mostly sent are each of the UAE with (4) requests, all related to the suspicion of money laundering, in addition to the USA with (3) requests, all related to money laundering as well.
- (17) information requests were sent during 2017. It was indicated that the countries to which requests were mostly sent are the UAE with (4) requests related to money laundering and terrorist financing, in addition to the Republic of Iraq with (3) requests, all related to money laundering.
- (27) information requests were sent during 2018. It was found that the countries to which requests were mostly sent are KSA by (4) requests, in addition to the Republic of Iraq and the UAE by (3) requests for each, all related to money laundering.
- (41) information requests were sent during 2019. It was noted that the countries to which requests were mostly sent are KSA with (12) requests, in addition to the Republic of Iraq by (8) requests, followed by the UAE with (5) requests, all related to money laundering.

**2. Incoming international cooperation requests of information:**

- The cooperation requests received by the Unit during 2016 were concentrated from each of the USA by (11) requests related to money laundering and terrorist financing, in addition to the Republic of Iraq and the UAE with (7) and (4) requests, respectively, all related to the suspicion of money laundering.
- The cooperation requests received by the Unit during 2017 were mainly from the USA by (10) requests related to money laundering and terrorist financing, in addition to each of Syria and Bahrain with (4) and (3) requests, respectively, all related to money laundering and terrorist financing.
- The cooperation requests received by the Unit during 2018 were concentrated from the Republic of Iraq with (27) requests related to money laundering, in addition to the USA with (8) requests related to money laundering and terrorist financing. (5) requests related to money laundering were also received from each of the Netherlands and Palestine.
- The cooperation requests received by the Unit during 2019 were coming mainly from the USA with (12) requests related to money laundering and terrorist financing, the Republic of Iraq by (11) requests related to money laundering, and Palestine with (7) requests related to money laundering.



**3. By examining the aforementioned figures and requests, the following has been revealed:**

- There is an increase in the requests issued by the Unit to counterpart entities, as they reached (16) requests in 2016 and rose to (41) requests in 2019. This indicates the increased awareness of the Unit in making more use of the information held by the counterpart units and strengthening international cooperation. It also reflects the benefit of joining international groups such as the Egmont Group.
- As for the issued cooperation requests, it is noticed that there was no significant difference regarding the number and content of the information requests issued by the Unit. However, the difference was associated with the countries from which the information was requested, as it was revealed that during 2017, the information was requested from counterpart units that were not dealt with during 2016; the most important of which were (Palestine, Lebanon and Sudan).
- There was a disparity in the quality of information provided by counterpart units in response to the information requests. However, most of these information were of great importance and were relied upon in the process of analyzing some related cases, such as the information received from each of (Iraq, Canada, and UK).
- As for the information requests received by the Unit, it is noted that the (USA, Iraq and Palestine) are the most countries sending cooperation requests.

**Forth: Trends**

- **According to the analyses made by the Unit to the notifications and suspicious reports it received, it is noted that the trends used by the criminals were concentrated in the following:**
  - a. Criminals tended to launder money obtained from the offences of tax evasion, fraud and physical across-border transportation, as the number of incoming notifications and reports related to these offences during the years 2016 and 2017 was a total of (426), while it reached (988) during 2018 and 2019, with an increase of (131.9%).
  - b. Tax evaders tended to use the formal financial sector in laundering money resulting from the tax evasion offence, especially banks, as it was found that they deposited money in their personal accounts instead of commercial bank accounts.
  - c. Criminals continued to exploit the banking sector for the purposes of laundering money obtained from the offences they committed. It was also noticed that the use of services provided by money exchange companies and electronic payment and collection services companies increased by criminals; this includes (money transfer services, electronic instruments, methods and financial services). In this regard, the number of notifications the Unit received from money exchange companies and payment and collection services companies during 2016 and 2017 was a total of (275), while it reached (392) notifications during 2018 and 2019, with an increase of (42.5%).

- d. Terrorist financiers tended to continue using the informal financial sector in the financing operations, in addition to their continued reliance on self-financing operations through personal loans, salaries and the sale of property.
- **Regarding the physical cross-border transportation of cash and bearer negotiable instruments:**

**After investigating cases related to non-declaration of across borders money transportation for the year 2019, the following has been found:**

1. There is a trend of cash smuggling, as it was found that the most frequent cases of non-declaration of funds are related to cash smuggling, which reached (34) cases during (2019), at (54%) of the total cases discovered. This is followed by a trend of cheque smuggling at a percentage of (28.5%) of total cases, and then the trend of smuggling gold and precious metals at (17.4%) of all cases.
2. All cases related to smuggling gold and precious metals were discovered specifically at the passengers airport, whereas the most frequent cases of cheque smuggling were made through the clearance airport center and the Capital's post office. As for cash smuggling, the most frequent cases were carried out through the land borders (Al-Omari, Jaber and Karameh), which indicates a trend of smuggling cash via land transport.

## **Fifth: Patterns and practical cases**

A set of patterns was identified based on the number of frequently occurring cases and the recurrent tendency of criminals in using a specific instrument or method to implement their plans. In order to enhance the quality of these patterns, they were determined based on the analysis of notifications and reports whose final results were to be referred to the jurisdiction or the security and supervision authorities, and on that they included convictions and imposition of sanctions. The following is a review of the most important of these patterns, with an indication of one practical case for each: -

### ***First pattern: Smuggling of gold and precious metals through the passengers airport***

#### **Summary of the practical case**

Hiding gold bars with one of the travelers coming to the Kingdom in order to pass them without being disclosed to the competent authorities upon arrival. The case was seized by the Jordan Customs Department, the bars were also confiscated, and a report was sent to the Unit.

#### **Summary of measures taken**

Pursuant to the provisions of Article (21) of the Anti-Money Laundering and Counter Terrorist Financing Law No. (46) of (2007) in force, the Unit has received two letters from the Jordan Customs Department being enclosed with the letter of the Director of the Passenger Airport Customs Center, together with its annexes which reveal that during the arrival of the so-called “M” of the Jordanian nationality from the state “W” through the Passenger Airport Customs

Center and upon inspection, non-declared (8.8) kilograms of gold with a value of (204,585) Jordanian dinars were found in his possession. In execution of the provisions of Article (21) of the AML/CTF Law in force, the customs department informed the Unit and referred the issue to it with all the annexes. The gold mentioned above has been also seized until the judicial decision is made in this case.

### **Annexes details**

- A copy of a letter by the Director of the Passenger Airport Customs Center issued to the Jordan Customs General Director indicating the dispatch of a parcel containing (8.8) kilograms of gold struck by the customs seal, and that the customs fines amounting to (51,299) Jordanian dinars incurred to the said person were collected under a financial receipt.
- A copy of the customs seizure report showing that the gold was seized while being concealed around the traveler's body and on his feet. Upon transfer, he stated that it is cigarettes.

### **The Unit's Procedures**

- By studying the annexes and referring to the Unit's database and the available commercial databases, it is found that the Unit did not have any negative information related to the said person till date.
- Accordingly, the Unit referred the issue to the Attorney General pursuant to the provisions of Article (21) of the AML/CTF Law in force with regards to the non-declaration of funds transported across borders. It also informed the Attorney General that it will finalize its investigation and financial analysis procedures in relation to the said person, and provide them later on with the results, upon completion.

### **The Unit has sent letters to complete its procedures as follows:**

- Issuing letters to all banks operating in the Kingdom requesting them to provide the Unit with the accounts belonging to the so-called "M" and the financial analysis of these accounts.
- Issuing letters to all major transfer agents of Western Union and MoneyGram to provide the Unit with the outgoing and incoming transfers related to the said person.
- Addressing the Preventive Security Department to provide the Unit with any criminal records detected against the so-called "M" and auditing them through the local, Arab, and international police databases and the travel movements of the said person.
- Addressing the General Intelligence Department to inquire about any negative security information regarding the said person.
- Addressing the counterpart unit in the country where the suspect came from to inquire about any information available regarding him and whether he declared any funds upon his departure.

**The responses to the unit's letters came as follows:**

- The counterpart unit responded that the said person works officially in the country, he is of a high income, does not have any accounts with banks operating in that country, there is no negative information about him, and he did not declare any funds in his possession upon his departure to Jordan.
- It is found that the said person has one outstanding account with a bank operating in the Kingdom, and that the financial transactions performed on his account were only crediting his pension salaries due to his previous service with the Jordanian official authorities.
- It is found that the said person received two internal remittances via "MoneyGram", with a total value of (200) Jordanian Dinars, and he also issued two internal remittances, amounting (250) Jordanian Dinars through "Western Union".
- The Unit noticed through the response of the Preventive Security Department that there are no criminal records against the said person, and he does have travel movements to the country (e), which is the same country from which he came when seized by the Jordan Customs Department in possession of the gold.
- It was revealed through the response of the General Intelligence Department that there was no negative security information against the said person.
- It was not evident that there were any suspicious financial transactions on the said person's account, or that he received any suspicious transfers.
- The Unit referred the findings of studying authorities' responses to the Attorney General in order to include them in the first referral and to enable them to take their own measures in accordance with the laws in force.

**The said person was convicted of the offense of bringing cash into the Kingdom whose value exceeds the mounts limit allowed to be entered without declaration in accordance with the provisions of Article (20 / a) of the AML/CTF Law, and was fined pursuant to the provisions of Article (25 / c) of the same law with a percentage of (10%) of the value of non-declared funds.**

*Second pattern: tax evasion by using the personal account for commercial purposes*

**Summary of the practical case:**

In this case, the personal account was used by a person to execute commercial financial transactions for one of the companies with which he is a partner in order to conceal these commercial transactions so that the Income and Sales Tax Department would not discover them.

**Summary of the measures taken:**

A notification was received to the Unit from a bank regarding the so-called (n), an owner of a large company, stating that the said person was using his personal bank accounts for carrying out his business instead of using his company accounts, which may indicate his violation of the Income and Sales Tax Law through tax evasion.

Another notification was also received later on from one of the banks regarding the so-called (m), the said person's brother and partner in the same company, for using his personal accounts for commercial purposes. It became clear to the bank that the account of the so-called (m) had witnessed intensive financial transactions in the form of cash deposits followed by foreign transfers, where the beneficiary was the account of the said person with a foreign bank.

**Results of the Unit's investigation and financial analysis procedures**

After completing the Unit's investigation and financial analysis procedures regarding the transactions made to the accounts of the so-called (N) and (M) during a period of approximately one year, and by requesting security information and referring to the available databases, the following was revealed:

- The family of the said persons owns a food company in the Kingdom and has several branches, in addition to their possession of a factory for the same purpose.
- The said persons are partners in four registered companies operating in this field.
- The volume of financial transactions credited to the accounts of the so-called (N) was equivalent to about (2.1) million Jordanian dinars, most of which were cash deposits made by employees in the company.
- The volume of financial transactions debited on the accounts of the so-called (N) was equivalent to about (2.2) million Jordanian dinars, most of which were represented by cheques and internal transfers.
- The volume of financial transactions credited to the accounts of the so-called (m) was equivalent to about (976) million Jordanian dinars, most of which were cash deposits made also by employees in the company.
- The volume of financial transactions debited on the accounts of the so-called (m) was equivalent to about (2.3) million Jordanian dinars, most of which were financial transactions in the form of foreign transfers and cheques drawn on the accounts whether in cash or through the clearing system.

- The sales returns are commensurate with the nature of the financial transactions executed on the accounts.
- The source of funds comes from the company's activity.
- The nature of the cycle of the financial transactions made on the personal accounts of the so-called (N) and (M) shows that the said persons make cash deposits for sales, and purchase goods from dealers under cheques.
- The financial transactions made on the personal accounts of the said persons with the bank are related to companies as well as persons owning individual institutions and are partners in different companies whose objectives are consistent with the nature of the activity of the said persons' companies.
- Accordingly, and since the said persons (N) and (M) clearly use their personal accounts for commercial purposes related to the work of the companies with which they are partners, which strongly indicates that they have committed the tax evasion offence, the Unit referred the two notifications to the Income and Sales Tax Department to carry out their own actions in accordance with the provisions of relevant legislation in force.

**The Unit received a letter from the Income and Sales Tax Department stating that, after making audits, it was found that there were violations by the so-called (N) of the provisions of the applicable income and sales tax laws that resulted in differences in the income and sales tax due on him, in addition to fines totaling about (11) million Jordanian dinars.**

*Third pattern: impersonation of princes from the Gulf countries to delude people for collecting donations to help the poor through social media channels*

### Summary of the practical case

In this case, a group of persons practicing fraud on social media channels was discovered as they requested funds to be transferred to them through money exchange companies, and they convinced the donors that they were collecting donations to help the poor on behalf of Gulf sheikhs and princes. The money exchange company received complaints from customers who have sent the remittances stating that they had been victims of fraud.

### Summary of the measures taken

The Unit received 6 notifications from a money exchange company stating that the so-called “x/ of an Arab nationality,” the so-called “p/ of an Arab nationality,” the so-called “o/ Jordanian,” and the so-called “e/ Jordanian”, the so-called “r/ Jordanian”, and the so-called “n/ Jordanian” received (31) foreign remittances, with a total value of (51,017) US dollars. The reporting company suspected that the said persons claimed via social media channels that they are sheikhs and princes of state (A) and that they are sending money to help the poor in the country (Y)

where people are asked to send money in exchange for freight rates and to release aid amounts. In addition, the reporting company received calls from some remittance senders demanding that their remittances be canceled because they are being exposed to fraud. The Unit has started to carry out its investigation procedures by referring to the available databases and commercial databases, in addition to the websites of "the Ministry of Industry, Trade and Supply" and "Companies Control Department". Besides, the following local authorities were also addressed:

- The "Preventive Security Department": to inquire about the said persons and whether there are any criminal records or lawsuits against them. The Department responded that there are many criminal records against the said persons, with the exception of both the so-called "x" and "p".
- All money exchange companies that have obtained approval to deal with the state (Y)" were requested to figure out whether the said persons have sent or received any remittances through them. All companies responded that said persons received (56) remittances with a value equivalent to (29,724) Jordanian dinars.
- By studying and analyzing the responses received from the rest of the money exchange companies that were addressed, the following was revealed:
  1. The total remittances received by the said persons were (87) remittances, with a total value equivalent to (80,741) Jordanian dinars.
  2. The said persons received split remittances from different senders.
  3. There is no real reliable relationship between the said persons and the remittance parties.
  4. The percentage of remittances received from state (Y) represents (60%) of the total remittances.
- The mechanism for receiving remittances by the said persons is similar, which indicates the existence of unknown person who is employing them in this work. In light of the difficulty in determining the beneficial owner of the remittances, in addition to the lack of a clear relationship between the said persons and the remittance senders, the issue was referred to the Preventive Security Department in accordance with the provisions of Paragraph (b) of Article (7) of the AML/CTF Law in force.

**The Unit received a feedback from the "Preventive Security Department" regarding the above issue stating that in light of the information received from the Unit, a network of several persons executing fraud through social media channels was captured. After investigation, the head of the network as well as the beneficial owners of the remittances were arrested and referred to court, which sentenced that the funds, subject of the crime, the tools used and the criminal proceeds to be confiscated, and that the said persons to be convicted of fraud and the offence of laundering money resulting from a misdemeanor.**



*Forth Pattern (terrorist financing): Collecting cash donations (Cash Fundraising) through social media channels without obtaining an official authorization:*

### Summary of the practical case

In this case, two people were found using a social media site to collect money in the name of “donations for the poor”, and they were using these funds for the purpose of financing and supporting the travel of fighters to the battlefields.

### Summary of the measures taken

- Through the intelligence follow-ups of one of the extremists, the so-called (x), by the General Intelligence Department, they reached to intelligence information about the existence of extremist activities related to the said person.
- The intelligence and financial follow-up of this extremist was expanded and information was requested from the AML/CTF Unit about his financial activities and accounts. The Unit was also asked to conduct financial analysis of the accounts of the said person, his origins (ancestors), and branches (descendants) for the purpose of expanding the search for the sources of his funds, along with their final destination.
- The AML/CTF Unit started its investigation procedures by referring to the available databases and commercial databases, in addition to the websites of the "Ministry of Industry, Trade, and Supply", the "Companies Control Department," and the Mizan website of the Ministry of Justice. Negative information was not found against the said person.
- The Unit requested all banks operating in the Kingdom and all transfer agents of Western Union, MoneyGram and Xpress Money to provide it with any information available on any accounts or transfers of the said person, his origins (ancestors), and branches (descendants) over a period of about one year. After completing the study of all responses, the following was revealed: -
  - ✓ The said person has a joint account with one of the persons, the so-called (s), with a bank operating in the Kingdom.
  - ✓ This account is mainly replenished through foreign remittances received from different countries, in addition to cash deposits and internal remittances from Jordanian money exchange companies, which deposit and transfer the amounts of remittances received by the said person to his joint bank account with the so-called (s) at his request.
  - ✓ By reviewing the details of the remittances received by the said person, along with the supporting documents provided to us by banks and money exchange companies, it is clear that the purpose of most of these transfers was (charitable donations to the poor and needy).
  - ✓ It was found that the said person (s) transferred part of the amounts available in the joint account to persons residing in one of the countries having conflicts and disorders. It was



also revealed that the said person (x) transfers another part of these amounts to persons located in different regions within the Kingdom.

- By tracing the page of the so-called (s) on a social media channel, it was found that he is using this page for the purpose of seeking people's sympathy and collecting donations, as he claims that he sends these donations to the poor and needy; he uploads pictures on his page to confirm this.
- After completing the Unit's investigation and financial analysis procedures, the General Intelligence Department was provided with the information and findings reached. The so-called (x) and (s) were arrested, and after an expanded investigation with them, it was found that part of the funds collected via the internet are disbursed in financing the travel of terrorists to battlefields, and another part is transferred to these terrorists after travelling in order to support them.
- Both of the said persons (x) and (s) were referred to court on charges of terrorist financing, as they were convicted and sentenced to hard labour for a period of (10) years, in addition to confiscating the funds in their joint account and their personal accounts.
- Cell phones, laptops, and a vehicle belonging to the said persons were also confiscated, as all of these tools were used to commit the terrorist financing offence.

### Sixth: indicators

A set of indicators related to money laundering and terrorist financing operations have been identified, and with the aim of increasing the quality of these indicators, their identification has been based on analyzing notifications and reports whose final results were to be referred to the court or competent security and supervisory authorities, taking into account that the indicators presented below do not constitute a comprehensive list of all ML and TF indicators; rather, they are only the most important ones:

#### ***ML indicators:***

- Existence of financial transactions of a commercial nature on the customers' personal accounts.
- Recurrent cash deposits and withdrawals, as well as deposit and issuance of cheques in a way that is not consistent with the nature of the activity declared by the customer.
- Cash deposits made to the account, followed directly by foreign transfers without a clear justification.
- Cash deposits frequently made to the customer's accounts by other people without a clear relationship between them.
- The absence of a clear relationship between the senders and beneficiaries of remittances, considering that there are recurrent remittances per person, with varying amounts that do not indicate a specific activity.

- Recurrent cash deposits with small amounts of money indicating that the customer splits large cash deposits to avoid accountability from the bank.
- Failure of the customer/s to provide the necessary supporting documents upon request.
- The customer behavior in terms of his/ her confusion and inability to answer the questions posed to him/ her by the reporting entity when performing the financial transaction, as a group of customers were using other people over the phone to answer the questions which indicates that they are not the beneficial owners.
- The customer's attempt to bribe the employee in order to submit his/ her transaction.
- Complaints received by the reporting entities from persons who have been defrauded with sums of money by other people impersonating Gulf sheikhs and princes.
- The existence of negative information about people published on the internet and through commercial websites such as (World-Check) and (Nexis Diligence).
- Forgery of documents or possession of forged documents.
- Receiving foreign remittances for the purpose of collecting donations without obtaining the necessary approvals from the concerned official authorities.
- Exchanging large amounts of small-denomination banknotes with large-denomination banknotes without a clear justification.
- Transferring funds to several beneficiaries residing in one region; the amounts are identical and the beneficiaries are different in each transfer.
- Engaging in activities without obtaining the necessary authorization or approval from the competent authorities, such as the money exchange business and collection of donations.
- Dormant accounts are activated by customers to receive foreign transfers with large amounts of money.
- The source of funds is not established.
- When the capital of a new company is deposited with a bank, the company's registration procedures are completed, and documents are obtained from the bank to deposit the capital, the deposited amount is withdrawn from the account, which indicates that it is a shell company or a front for other purposes.

***Terrorist financing indicators:***

- Selling personal property suddenly and without a clear justification.
- Exploiting the presence of the Syrian community in the Kingdom for the purpose of collecting funds in their name and disclosing that these amounts are used for providing aids to them.
- Fundraising without an authorization.
- Receiving donations/ remittances from different countries with no clear relationship and without obtaining the necessary approvals from the competent authorities.
- Using different technology tools for making money transfers and changing the IP address to hide the tracking features.
- The name of the account holder appeared on the terrorists lists.
- Using ATM cards and credit cards in high-risk countries or in border areas of high-risk countries.
- Non- declaration or false declaration of funds transported across borders.
- Transfers from and to conflict areas, high-risk countries or their neighboring states are recurrent and at low values.
- The customer visits a branch of a financial institution far from his/ her place of residence and work, and does not provide a clear justification for choosing this branch.
- Having several accounts with the bank for different individuals who do not have any relationship, except that these accounts have common addresses (the same phone number, residence, apartment address and mailbox).
- The customer frequently changes his/ her place of residence.
- The customer's concern and confusion, failure to provide solid justifications, and inability to explain the reason for the financial transfer, the sender, or the purpose of the financial activity.
- Cash deposits with one of the bank's branches, followed directly by cash withdrawals from the ATM from places relatively far from the place of deposit, or from places where extremist organizations exist or those close to conflict areas.
- Using the ATM card and credit cards to execute unusual purchases of chemicals used in the manufacture of explosives without any commercial activity that justifies the reason for purchasing such materials.
- Using the ATM card and credit cards to buy airline tickets for countries in conflict zones or their neighboring countries.
- Getting life insurance policies despite the customer's young age.

- Executing financial transactions on the account after a long period of being inactive or dormant.

## Seventh: Recommendations

- Increasing the effectiveness of designated non-financial businesses and professions in combating money laundering and terrorist financing, and raising awareness of these entities due to the slight number of notifications received from them.
- Despite the high number of notifications received from money exchange companies throughout the study period, it does not reflect the size of this sector within the Kingdom, as most money exchange companies did not report any suspicious transaction. However, it is noted that the companies who have sent the notifications are considered one of those who are widely spread in various regions of the Kingdom and have a large customer base compared to the rest of companies that did not send notifications to the Unit.
- By examining the notifications received from money exchange companies, it is found that there were cases in which refugees, the low economic status, and unemployment were exploited, whether by others or through the refugees themselves, as it was noted that the mechanism of requesting personal and family financial aids to collect money through various financial transfer systems was clearly spread, which indicates the need to impose stricter supervision by money transfer companies and money exchange companies on the remittance movements they execute, especially the ones issued and received from countries witnessing armed conflicts or where terrorist organizations exist, in addition to adopting a risk-based approach and intensifying the inspection rounds by supervisors in the field of combating money laundering and terrorist financing.
- Continuing efforts to detect those involved in the activity of transferring funds in an unauthorized way and imposing dissuasive sanctions against them.
- The need to enhance and raise awareness of the security authorities to make greater use of the referrals they receive from the Unit regarding suspicious financial transfers, in light of the fact that most of the suspects indicated in the notifications are not the beneficial owners of these transfers.
- Constantly providing the feedback and conducting meetings with banks in order to improve the quality of the notifications received from them, as it was clear that the objective behind some of these notifications is requiring banks to adopt the defensive SARs policy, or that these notifications occurred after the suspect closed the account with the bank.
- The aforementioned data reveals that the Jordanian society is considered one of the societies based on monetary financial transactions, which indicates the need to work on reinforcing financial inclusion and linking the financial transactions that customers make to their accounts with banks or through electronic portfolios to determine the source of money and wealth, and to trace their final destination and the ultimate beneficial owners.

- Increasing the effectiveness of relevant laws and legislations so that they are more effective and have greater impact through the implementation of international recommendations and standards.

---

Anti Money Laundering & Counter Terrorist Financing Unit

[www.amlu.gov.jo](http://www.amlu.gov.jo) Website:

e-mail: [info@amlu.gov.jo](mailto:info@amlu.gov.jo)