

THE FCIB PUBLISHES TWO NEW SUSPICIOUS TRANSACTION REPORTING GUIDELINES

I. INTRODUCTION

The Financial Crimes Investigation Board (the “FCIB”) published the Guidelines on the Detection and Suspicious Transaction Reporting of Hawala and Similar Alternative Value Transfer Systems (the “**Hawala Guidelines**”) on September 11, 2026, and the Guidelines on Suspicious Transaction Reporting for Combating Money Mule Accounts (the “**Money Mule Account Guidelines**”) on October 13, 2026. These guidelines provide important explanations regarding the identification and prevention of risks arising from the use of financial accounts by third parties and from hawala and similar alternative value transfer systems, within the framework of combating money laundering and terrorist financing.

The guidelines address matters such as the procurement and management of money mule accounts, their use in illegal payment and collection infrastructures, the transfer of economic value among different persons, accounts, and asset types, and the identification of the beneficial owners of such transactions. They also set out key risk indicators for different categories of obliged entities and provide guidance on the identification and reporting of suspicious transactions, as well as the preventive measures to be adopted.

1. Concepts of Hawala and Money Mule Accounts

The Hawala Guidelines describe hawala and similar alternative value transfer systems as arrangements whereby funds or economic value delivered in one location are made available to another person or at another location without requiring a direct transfer of such funds or value. These systems essentially involve three stages: (i) the acceptance of funds or economic value, (ii) the delivery of the corresponding value at another location, and (iii) the subsequent settlement of receivables and payables among intermediaries. Settlement among intermediaries may be carried out separately following each transaction or through the offsetting of transactions conducted in different directions, with only the net balance ultimately being settled.

The Money Mule Account Guidelines define the use of money mule accounts as the use of financial accounts belonging to natural or legal persons by third parties or by the account holders themselves acting under the direction of such third parties. This practice is not limited to making bank accounts available to third parties in exchange for compensation and may take various forms. In this context, examples of money mule account arrangements include the transfer of bank account access credentials to third parties, the execution of transactions by account holders in accordance with third-party instructions, and the use of corporate accounts to collect payments on behalf of third parties.

Although money mule account arrangements and hawala systems operate through different mechanisms, both practices make it more difficult to identify the true source of funds, the parties involved in transactions, and the ultimate beneficiaries. In particular, the use of accounts belonging to third parties to collect or distribute funds or convert them into different types of assets may give rise to risks associated with the operation of hawala-like alternative value

transfer systems. Accordingly, it is important to assess these practices together within the framework of preventing money laundering and terrorist financing.

2. Illegal Payment Infrastructures, Shell Companies, and Hawala Systems

The Money Mule Account Guidelines explain that money mule accounts may be used as part of organized payment and collection systems rather than merely for isolated transactions. In particular, activities involving illegal betting, gambling, and investment fraud may entail the collection of funds through accounts belonging to different natural and legal persons, the distribution of such funds to other accounts, and their eventual conversion into different financial instruments. Within such structures, numerous accounts may be used as part of centrally managed collection pools, funds may be transferred to different financial institutions within short periods, and payment processes may be managed automatically through API connections.

The Money Mule Account Guidelines also draw attention to specific risks associated with shell companies and companies that are acquired and reactivated after prolonged periods of inactivity. In particular, transaction volumes that are inconsistent with a company's business activities, financial capacity, and commercial history, as well as discrepancies between its nominal shareholders and those exercising actual management control, are considered significant risk indicators.

The use of money mule accounts in organized collection and distribution networks may also give rise to risks associated with the alternative value transfer systems addressed in the Hawala Guidelines. In hawala and similar systems, the equivalent value of funds collected from different persons may be made available to other persons or at other locations without requiring the direct transfer of the same funds, while receivables and payables among intermediaries may subsequently be offset against one another. In this context, money mule accounts may be used to collect or distribute funds or convert them into different types of assets within hawala-like systems.

3. Legal Consequences of the Use of Money Mule Accounts

The Money Mule Account Guidelines indicate that the use of money mule accounts may fall within the scope of different criminal offenses depending on the circumstances of each case. In this regard, the following provisions are particularly relevant:

- **Failure to disclose transactions conducted on behalf of another person:** Pursuant to Article 15 of Law on the Prevention of Laundering Proceeds of Crime (Law No. 5549) (the “**Law No. 5549**”), persons who act in their own name but actually conduct transactions on behalf of another person in transactions requiring identification must notify the obliged entity in writing, prior to the transaction, of the person on whose behalf they are acting. Failure to comply with this obligation is punishable by imprisonment for a term of six months to one year or a judicial fine of up to five thousand days.

- **Laundrying of assets derived from criminal activities:** Under Article 282 of the Turkish Criminal Code (Law No. 5237) (the “TCC”), the use of money mule accounts to conceal the source of proceeds of crime, transfer such proceeds to different accounts, or give them an appearance of legitimacy may, depending on the specific circumstances of the case, be assessed under the provisions governing the offense of money laundering.
- **Fraud and illegal betting activities:** The use of money mule accounts to collect proceeds from fraudulent activities or as part of payment infrastructures for illegal betting and gambling activities may give rise to legal and criminal liability under the provisions of the TCC governing fraud and gambling, as well as Law on the Regulation of Betting and Games of Chance in Football and Other Sports Competitions (Law No. 7258), depending on the nature of the acts concerned.
- **Terrorist financing and circumvention of sanctions:** The use of money mule accounts to collect and transfer funds for terrorist financing purposes or to circumvent asset freezing measures may be subject to assessment under Law on the Prevention of the Financing of Terrorism (Law No. 6415).

The Money Mule Account Guidelines further state that where money mule accounts are procured and used in an organized manner, the provisions of Article 220 of the TCC governing the establishment of an organization for the purpose of committing crimes may also become applicable.

Where transaction patterns associated with hawala are identified, the provisions of Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (Law No. 6493) concerning the provision of unauthorized payment services may also become applicable, depending on the nature of the services actually provided, together with other relevant criminal and sanction provisions, as warranted by the specific circumstances of the case.



4. Key Risk Indicators for Identifying Money Mule Accounts

The Money Mule Account Guidelines emphasize that identifying the use of money mule accounts requires an assessment of transaction patterns, connections between accounts, and the consistency between customers' economic profiles and transaction behavior, rather than focusing solely on individual transactions. In this context, key risk indicators include customers conducting high-volume transactions that are inconsistent with their financial capacity or business activities, receiving funds from numerous unrelated persons within a short period and subsequently transferring those funds to other accounts, and the management of seemingly independent accounts through shared technical infrastructure or access credentials. Other factors to be considered when assessing suspicious transactions include newly established companies or companies reactivated after prolonged periods of inactivity conducting transactions that are inconsistent with their business capacity, the concentration of funds in certain accounts, customers' inability to provide adequate explanations regarding the purpose of transactions and the source of funds, and the conversion of funds into different financial instruments without an identifiable economic rationale.

The Hawala Guidelines, in turn, draw particular attention to the identification of economic connections between seemingly unrelated transactions and the risks associated with the movement of funds through different persons, accounts, and asset types. In this context, key risk indicators include fund transfers to the same recipient by persons with no apparent economic relationship, the splitting and transfer of funds through multiple accounts, the rapid conversion of substantial funds received from abroad into cash or other assets, and continuous movements of funds between bank accounts and crypto asset wallets. Furthermore, the offsetting of transactions involving different customers and the availability of economic value to other persons or at other locations without a direct transfer of funds may make it more difficult to determine the true economic substance of such transactions.

The Money Mule Account Guidelines also recommend assessing these indicators through the use of network analytics, advanced data analytics, anomaly detection, and artificial intelligence-based tools. In this regard, it is important for compliance departments not to rely solely on controls based on predefined transaction scenarios, but also to develop monitoring mechanisms capable of identifying common behavioral patterns and connections between seemingly unrelated accounts.

5. Measures to Be Taken Prior to Suspicious Transaction Reporting

The Money Mule Account Guidelines set out the measures to be taken by obliged entities where suspicions arise regarding the use of money mule accounts. The FCIB expressly emphasizes that filing a suspicious transaction report alone does not constitute a sufficient measure and that the primary objective is to prevent the continued use of the suspicious account for illegal activities. Accordingly, pursuant to the Law No. 5549 and the relevant secondary legislation, obliged entities are required to consider the following measures depending on the nature of the risk:

- **Customer due diligence and enhanced review:** Examining the customer's economic and business activities, transaction volumes, source of funds, purpose of

transactions, and beneficial ownership, and requesting additional information and documentation from the customer where necessary.

- **Contacting the customer:** Determining whether the customer is aware of the transactions, identifying the person actually operating the account, and establishing the nature of any existing relationships with third parties.
- **Transaction and access restrictions:** Depending on the circumstances of the case, reducing transaction limits, restricting certain products and services, limiting access to mobile or internet banking, suspending POS and virtual POS services, or restricting transfers to external wallets.
- **Assessment of the business relationship:** Declining to execute transactions and, where necessary, terminating the business relationship if the risk cannot be adequately managed through the measures adopted, the customer's explanations remain insufficient, or it is determined that the account is being used by third parties.
- **Content of suspicious transaction reports:** Ensuring that suspicious transaction reports are not limited to technical summaries of transaction activity, but also include explanations obtained from the customer, supporting documentation, examinations conducted, and inconsistencies identified.

Particularly for financial institutions operating exclusively through digital channels, access restrictions are expected to be implemented progressively, taking into account the institution's service model and the level of risk involved. The Money Mule Account Guidelines state that failure to adopt the necessary preventive measures despite the presence of clear risk indicators associated with the use of money mule accounts may expose obliged entities to administrative sanctions and, depending on the specific circumstances of the case, may also give rise to criminal proceedings. Nevertheless, a mere breach of administrative obligations or the existence of objective risk indicators does not, in itself, give rise to criminal liability. In assessing criminal liability, the knowledge, intent, and involvement of the relevant persons in the conduct concerned must also be taken into account.

6. Key Regulatory Considerations and Risk Indicators by Sector

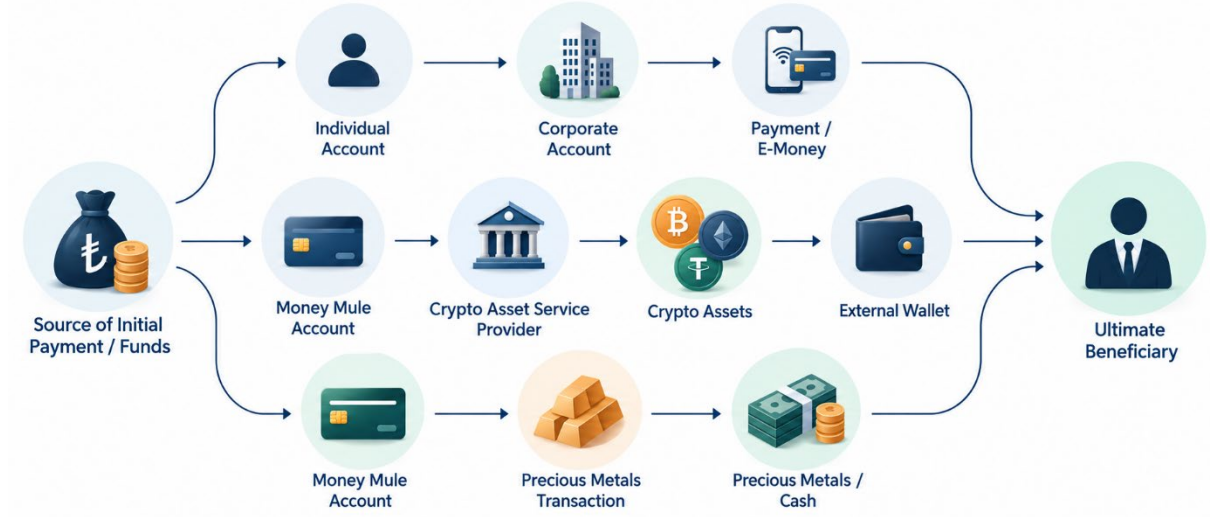
The Money Mule Account Guidelines identify sector-specific risk indicators associated with the use of money mule accounts across nine categories of obliged entities.

Sector	Key Risks
Banks	Accounts operated by third parties, high-volume and rapid fund transfers, shared technical access credentials, account rotation, and shell companies.

Payment and Electronic Money Institutions	Collection of funds from numerous accounts, rapid transfers through FAST, use of shared devices and IP addresses, and misuse of POS and virtual POS transactions.
Crypto Asset Service Providers	Conversion of funds originating from money mule accounts into crypto assets, transfers to connected external wallets, and transactions inconsistent with customer profiles.
Authorized Foreign Exchange Institutions	Foreign exchange transactions funded through third-party accounts and conversion of funds into cash or foreign currency on behalf of different persons.
Jewelers and the Precious Metals Sector	Purchases of precious metals using funds received from third-party accounts and transfers of proceeds to persons with no identifiable economic relationship.
Capital Markets Brokerage Firms	Investment accounts funded by third parties, securities transfers without an identifiable economic rationale, and movements of funds between connected accounts.
Certified Public Accountants and Sworn-in Certified Public Accountants	Companies lacking genuine economic activity, financial transactions inconsistent with their business activities, and discrepancies between nominal shareholders and persons exercising actual management control.
Notaries	Broad powers of attorney granted to the same persons, recurring company incorporation and share transfer transactions, and the granting of financial authority to third parties.
Attorneys	Establishment of shell companies, concealment of beneficial ownership, and authorizations relating to company transfers and financial transactions.

The Money Mule Account Guidelines further identify crypto asset service providers as critical points of transition within the financial system for converting funds collected through money mule accounts into different types of assets and transferring them to external wallets. In this context, the Guidelines particularly emphasize the need to examine, in conjunction, the relationship between customers' bank accounts and crypto asset accounts, the devices and access credentials used, transfers to external wallets, and transactions inconsistent with customers' financial profiles.

Both Guidelines also draw attention to transaction patterns aimed at circumventing the transfer restrictions and transaction limits imposed under the Financial Crimes Investigation Board General Communiqué Serial No. 29. In particular, the use of different crypto assets as intermediary assets to avoid limits applicable to stablecoins may constitute a risk indicator depending on the specific circumstances of the case. Accordingly, it is important for crypto asset service providers to review their existing monitoring and control systems to ensure that customer accounts, sources of funds, technical access credentials, and transaction relationships on the blockchain are assessed collectively.



II. CONCLUSION

The Hawala Guidelines and the Money Mule Account Guidelines published by the FCIB highlight the importance of shifting from an approach focused on individual transactions and accounts to a risk-based monitoring and control approach involving a comprehensive assessment of financial networks and movements of economic value in combating money laundering and terrorist financing. In this context, identifying money mule accounts and hawala and similar alternative value transfer systems requires an assessment not only of account activity but also of the sources of funds, connections between transaction parties, conversions between different asset types, and ultimate beneficiaries.

Integrating the sector-specific risk indicators set out in both Guidelines into existing compliance programs, strengthening customer onboarding and identification procedures, enhancing transaction monitoring mechanisms, and establishing controls specifically designed to identify connections between accounts controlled by third parties and seemingly unrelated transactions are essential for ensuring regulatory compliance and mitigating potential legal risks for obliged entities. Accordingly, compliance with suspicious transaction reporting obligations does not relieve obliged entities of their other obligations relating to customer due diligence, risk management, monitoring and control, and the implementation of necessary preventive measures.

Finally, it should be noted that the risk indicators set out in the Hawala Guidelines and the Money Mule Account Guidelines do not replace other the FCIB guidelines issued for the relevant sectors but are intended to complement them. Therefore, obliged entities must conduct their assessments in conjunction with the applicable legislation and sector-specific guidelines currently in force in their respective areas of activity.

This legal update has been prepared in accordance with the general principles of Turkish law and in light of developments up to October 2, 2026, solely for general informational purposes. It does not constitute promotional or advertising material or an assessment of any specific circumstances. Accordingly, the information contained

VARDAR | ŞANLI

herein may vary depending on the particular circumstances of each case, and Vardar Şanlı Law Firm shall not be held liable in respect of such circumstances.