ERYÜREKLİ

**Briefing Note**
Capital Markets
30 June 2026

# Obligations of Crypto Asset Service Providers Regarding the Prevention of Financial Crimes

Mustafa Adıgüzel, Associate
Sıla Ustaoğlu, Associate

*Certain mandatory obligations have been introduced under international and domestic legislation for specific commercial and professional organizations, particularly financial institutions, to prevent financial crimes such as money laundering and the financing of terrorism; and the authority and duty to regulate and supervise this field in Türkiye has been granted to the Financial Crimes Investigation Board ("**MASAK** or **FCIB**").*

*In this context, the Law on Prevention of Laundering Proceeds of Crime No. 5549 ("**Law**"), the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Regulation on Measures**") and the obligations referred to in the relevant legislation determine the entities that hold the status of "obliged party" and bear the responsibility for compliance.*

*Crypto Asset Service Providers ("**CASPs**") are also listed among the entities holding the status of "obliged party" pursuant to the Law and the Regulation on Measures. In addition, the amendment made to the Regulation on Measures in 2024 classified CASPs under the status of "financial institution" and included them among the obliged parties required to establish a compliance program under the Regulation on Compliance Program Regarding Obligations on Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Regulation on Compliance**").*

*This briefing note has been prepared for your information to provide our explanations regarding the responsibilities that CASPs are required to comply with within the framework of MASAK regulations.*

# 1. Obligation to Know Your Customer

## 1.1. Identification

Pursuant to the Law, CASPs must identify those who conduct transactions and those on whose behalf or account transactions are conducted, within the scope of Know Your Customer ("**KYC**") principles, for transactions carried out before them or in which they intermediate. The identification process must be completed before establishing a business relationship or executing a transaction.

The framework agreement to be signed by CASPs with their customers is considered the beginning of a continuous business relationship. In this case, the obligation to obtain and verify the customer's identity information arises. In cases other than the establishment of a continuous business relationship, under the following circumstances:

- Regardless of the amount, in cases requiring a suspicious transaction report and when there is doubt about the adequacy and accuracy of previously obtained customer identity information, or

- When the transaction amount (*crypto asset or fiat currency*) or the total amount of multiple linked transactions is 15,000 TL or above,

CASPs are obliged to take the necessary measures to determine the beneficial owner of the transaction in addition to identity identification, and they may use the remote identification method, except for certain services. In the event that a previously conducted identification is doubted and the information cannot be verified, the business relationship with the customer is terminated, and an assessment is also made regarding whether the situation constitutes a suspicious transaction.

## 1.2. Travel Rule

For crypto asset transfers in an amount of 15,000 TL or above, it is mandatory to include the required and accurate information regarding the sender and the required information regarding the recipient in the transfer messages, and to transmit this information by preserving it in the relevant messages throughout

the transfer chain. The information regarding the sender and the recipient must be sent simultaneously with the transfer, and in the event that CASPs detect missing information, they must request the completion of this information from the sending CASPs.

### 1.3. Enhanced Measures

CASPs are obliged to apply enhanced measures in high-risk situations identified through a risk-based approach, in proportion to the identified risk. There are additional enhanced measures in four main areas specified by financial crimes legislation:

- **In Customer Relations:** Information regarding the source of funds and the purpose of the transaction must be obtained, and the business relationship must be kept under close monitoring. In high-risk situations, measures such as obtaining additional information, senior management approval, and requiring the first financial transaction to be made from another financial institution must be implemented.

- **In Crypto Asset Transfers:** Withdrawal transactions made to unhosted wallets or offshore CASPs without any obligations must be executed after a certain period (*72 hours for the first withdrawal, 48 hours for subsequent ones*) after the purchase/deposit transaction of the transferred asset. Daily/monthly limits (*3,000/50,000 USD*) must be applied for stable crypto assets, and a transaction description of at least 20 characters must be requested for transfers.

- **For Politically Exposed Persons:** Reasonable measures must be taken to identify these persons; senior management approval, determination of the source of funds, and close monitoring are mandatory in relations with foreign or high-risk domestic/international officials. The measures must continue for at least one year after leaving the duty.

- **In Remote Identification:** CASPs must conduct a risk assessment and obtain additional information such as the purpose of the business relationship, source of funds, and estimated transaction volume. The first financial transaction must be made from an account at another financial institution

where the principles regarding KYC are applied. Those intermediating in the trading of privacy-based crypto assets cannot conduct remote identification.

## 2. Monitoring and Reporting Obligations

### 2.1. Suspicious Transaction Reporting

CASPs must report transactions involving any information, suspicion, or grounds to suspect illegality to the MASAK Presidency using a Suspicious Transaction Report Form, without any monetary threshold. Following an investigation within the scope of powers and capabilities, the report must be submitted within ten business days at the latest from the date the suspicion arises (*or immediately if delay is detrimental*). The obliged party and its employees making the report are exempt from civil and criminal liability. The information that a report has been made cannot be disclosed to anyone, including the parties to the transaction, except in cases of judicial proceedings and audits.

### 2.2. Continuous Reporting

All obliged parties, including CASPs, must report transactions to the MASAK Presidency that exceed the amounts to be determined by the Ministry of Treasury and Finance ("**Ministry**"), out of the transactions to which they are a party or in which they intermediate. Interlinked transactions are considered a single transaction, and these notifications are generally carried out electronically, in accordance with the procedures and principles determined by the Ministry.

### 2.3. Suspension of Transactions and Freezing of Assets

The Ministry has the authority to suspend or prevent the execution of transactions involving suspicion of money laundering or terrorism financing for a period of seven business days for the purpose of verification and analysis. In the presence of serious indications supporting the suspicion, CASPs must submit a Suspicious Transaction Report to the MASAK Presidency along with a request for the suspension of the transaction. Following the request, executing the transaction must be abstained from until the decision of the Ministry is notified to them. The suspension period shall not exceed seven business days in any case.

CASPs are obliged to immediately implement asset freezing decisions published in the Official Gazette aimed at preventing the financing of terrorism and weapons of mass destruction, upon receiving a notification from MASAK, in order to prevent the dissipation of assets. CASPs holding assets before them must report the information regarding the frozen assets to MASAK within seven days, and they must exercise any authority of disposal over these assets solely upon an authorization document to be issued by MASAK.

## 3. Corporate Structure, Audit, and Sanctions

### 3.1. Compliance Program

CASPs must establish a compliance program focusing on a risk-based approach for the purpose of preventing the laundering of proceeds of crime and the financing of terrorism. The board of directors is ultimately responsible for the effectiveness of this program.

The compliance program consists of the following five main measures:

(i) **Corporate Policy and Procedures:** The written framework containing risk management, control, training, and internal audit policies.

(ii) **Risk Management Activities:** The methods for identifying, rating, and mitigating customer, service, and country risks.

(iii) **Monitoring and Control Activities:** The continuous review of high-risk transactions and customer profile compatibility.

(iv) **Training Activities:** Annual programs aimed at increasing regulatory compliance and risk awareness of personnel.

(v) **Internal Audit Activities:** The annual examination of the adequacy of policies and activities.

CASPs must appoint a compliance officer and a deputy compliance officer reporting to the board of directors to execute the compliance program. The primary responsibilities of the compliance officer are to coordinate regulatory

compliance, prepare corporate policies, execute risk management, and investigate suspicious transactions to report them to the MASAK Presidency.

### 3.2. Information and Notification

- **Obligation to Provide Information and Documents:** CASPs must provide all kinds of information, documents, and records requested by the MASAK Presidency fully, accurately, and within the requested period without delay, and they must keep their ledgers and information processing systems ready for audit during on-site inspections.

- **Obligation of Retention:** It is mandatory to retain documents regarding identification (*from the date the account is closed or the last transaction date*), ledgers, and all records of transactions for a period of eight years, and they must be submitted to competent authorities upon request.

- **Obligation of Notification:** It is essential that notifications to be made to CASPs are executed electronically through the system established by the MASAK Presidency. These notifications are deemed served when they reach the counterparty, and responses must also be sent electronically through the same system.

### 3.3. Protection of the Obliged Party

Information regarding those who make a suspicious transaction report cannot be provided to third parties, institutions, or organizations outside the court, and real persons and legal entities fulfilling their obligations in general shall in no way be held civilly or criminally liable.

### 3.4. Audit and Sanctions

Compliance of CASPs with the legislation is determined through audit of compliance with obligations and inspection of obligation violations. Administrative fines are imposed or the matter is referred to judicial authorities, depending on the nature of the violation, regarding CASPs for which a violation is detected as a result of the audit.

The general rule in determining the fine amount for transaction-based fines is that it is applied as two times the transaction amount, not to be less than five percent of the transaction amount.

Administrative fines imposed on CASPs if deficiencies are not remedied in the event of non-compliance with the compliance program obligation shall be applied to the board member responsible for the matter, or if none, to the senior executive, at a rate of one-fourth.

## 4. Conclusion

Obligations prescribed for CASPs within the scope of MASAK legislation are not limited solely to measures regarding the customer but necessitate a holistic compliance approach encompassing the internal organizational structure, process management, and technological infrastructure. Operating activities of CASPs within a risk-based compliance framework is of paramount importance, as non-compliance with these obligations may lead to high-amount administrative fines and additional sanctions.

***

*Should you have any queries on the matters above, please do not hesitate to contact us.*

*Yours faithfully,*

***Eryürekli Law Office***
*www.eryurekli.com*
*info@eryurekli.com*
*+90 212 365 9600*