

MODULE 3 — PREVENTING MISUSE OF VIRTUAL ASSETS: FRAUD PREVENTION & DUE DILIGENCE

ERCM Jean Monnet Module — Legal Regulation of Crypto-Assets: From Basics to Advanced

Grant Agreement No. 101126839 · Yaroslav Mudryi National Law University

In this module, we will examine the risk-based approach to preventing the misuse of virtual assets, the main types of fraud in this area, the principles of customer due diligence in virtual asset transactions, and the specific risks of P2P payments and exchanges. The sections below examine these questions in turn.

THE RISK-BASED APPROACH TO PREVENTING THE MISUSE OF VIRTUAL ASSETS

3.1. Concept and Principles of the Risk-Based Approach

The risk-based approach (RBA) is a foundational methodological principle of the international anti-money laundering and counter-terrorist financing (AML/CFT) system, enshrined in FATF Recommendation 1. Its essence is that states, regulators, and reporting entities — including virtual asset service providers (VASPs/CASPs) — must identify, assess, and understand the money laundering and terrorist financing risks inherent in their activities, and apply measures proportionate to the level of those risks.

Unlike a purely formal, checklist-based approach, the risk-based model allows compliance functions to concentrate limited resources where risks are highest, while applying simplified measures where risk is low. This is particularly relevant for the virtual asset market, characterized by high transaction speed, the cross-border nature of operations, potential pseudonymity, and the use of a broad range of technological solutions (wallets, mixers, DEXs, cross-chain bridges).

Components of Risk Assessment

- Customer risk — client status (PEP, beneficial owner, legal entity with a complex ownership structure), reputation, transaction history.
- Product/service risk — privacy-enhancing cryptocurrencies (privacy coins), mixers/tumblers, unhosted wallets, crypto-asset derivatives.
- Geographic risk — high-risk jurisdictions under FATF lists, sanctioned jurisdictions, countries with weak AML/CFT regimes.
- Delivery channel risk — remote identification without face-to-face contact, use of intermediaries, P2P platforms.

Based on a comprehensive assessment of these components, a reporting entity determines the appropriate level of customer due diligence: Simplified Due Diligence (SDD) for low-risk relationships, standard Customer Due Diligence (CDD) for typical cases, and Enhanced Due Diligence (EDD) for higher-risk customers or transactions.

National and Sectoral Risk Assessments

FATF Recommendations require states to conduct a National Risk Assessment (NRA) covering the virtual asset sector as well. Based on the NRA, regulators issue sectoral guidance for VASPs/CASPs on typical indicators of suspicious activity characteristic of crypto-asset transactions specifically: structuring transfers below reporting thresholds, rapid movement of funds through multiple wallets ("chain hopping"), use of mixers immediately after receiving funds, and conversion into privacy coins without an apparent economic purpose.

MAIN TYPES OF FRAUD INVOLVING VIRTUAL ASSETS

3.2. Typology of Fraud in the Virtual Asset Space

The rapid growth of the virtual asset market has been accompanied by the emergence of specific forms of fraud that combine classic social engineering techniques with the particular features of crypto-asset settlement (irreversibility of transactions, the absence of a central authority able to reverse a transfer, and the difficulty of identifying the recipient).

Carding

Carding involves the unlawful use of payment card data (card number, expiry date, CVV code) obtained through data breaches, phishing, or compromised payment systems, in order to purchase crypto-assets or top up accounts on crypto exchanges. The crypto-assets thus obtained are quickly moved through a chain of wallets or converted into other assets to break the paper trail. Carding poses a significant operational risk for CASPs, since once the fraud is detected the card issuer initiates a chargeback, while the crypto-assets may already have been withdrawn from the platform.

Phishing

Phishing consists of creating fake websites, emails, or messages that imitate official resources of crypto exchanges, wallets, or projects, in order to obtain private keys, seed phrases, or user credentials. A variant is spear-phishing — a targeted attack on a specific individual (for example, a project founder or an exchange employee) using personalized information — as well as clone-phishing, where the attacker copies a legitimate resource and changes only the recipient's payment details.

Vishing

Vishing is voice-based fraud in which the attacker calls the victim, posing as a representative of a crypto exchange's support service, a bank, or a law enforcement agency, and under the pretext of "protecting funds" or "confirming a transaction" persuades the victim to transfer crypto-assets to an address controlled by the fraudster, or to disclose confidential access credentials to a wallet or exchange account.

Scamming

Scamming covers a wide range of fraudulent schemes, including: investment fraud (promises of guaranteed returns from "trading platforms" or "mining pools"); romance combined with investment fraud ("pig butchering" — a prolonged trust-building process followed by persuading the victim to deposit funds into a fake trading platform); rug pulls — developers of a token or DeFi protocol

withdrawing liquidity immediately after raising investor funds; fake ICOs/IEOs/IDOs and airdrop scams, where victims seeking "free" tokens are asked to connect their wallet to a malicious smart contract and grant unlimited spending approval.

A common feature of these typologies is the exploitation of the irreversibility of blockchain transactions and the cross-border nature of the operations to make recovery through traditional civil or criminal procedural means practically impossible, which increases the importance of preventive measures at the stage of establishing a business relationship and of ongoing transaction monitoring.

DUE DILIGENCE IN VIRTUAL ASSET TRANSACTIONS

3.3. Customer Due Diligence in the Virtual Asset Market

Customer Identification and Verification (CDD)

The standard customer due diligence procedure involves establishing and verifying the customer's identity against official documents, identifying the beneficial owner for legal entities and trust-like arrangements, ascertaining the purpose and intended nature of the business relationship, and screening the customer against sanctions lists, PEP registers, and adverse media databases. In the virtual asset space, this procedure is supplemented by verification of the origin of the crypto-assets (source of funds/source of wealth) using blockchain analytics tools.

Enhanced Due Diligence (EDD)

Enhanced due diligence applies to higher-risk customers — PEPs, customers from high-risk jurisdictions, large transactions involving unhosted wallets, and cases where indicators of suspicious activity have been identified. EDD requires obtaining additional documentation on the source of funds, senior management approval for establishing the business relationship, and enhanced ongoing monitoring of the customer's transactions.

Transaction Monitoring and Blockchain Analytics

Ongoing monitoring of customer transactions is an integral part of CDD/EDD and involves detecting atypical patterns: structuring amounts to artificially avoid reporting thresholds; transactions with addresses linked to darknet marketplaces, sanctioned entities, or known fraud schemes (as identified by commercial blockchain analytics solutions); and a sharp increase in the volume or frequency of transactions without economic justification. Detected suspicious transactions are subject to internal investigation and, where grounds exist, a suspicious activity report to the financial intelligence unit.

The Travel Rule (FATF Recommendation 16)

The Travel Rule, set out in FATF Recommendation 16 and implemented in EU law by Regulation (EU) 2023/1113, requires CASPs transferring virtual assets to accompany the transaction with information about the originator and the beneficiary (name, account number/wallet address, and, for transfers above a set threshold, additional identifying data), regardless of the transfer amount within the EU. This directly extends to the virtual asset sector a principle that has applied to bank wire transfers for decades, and it is a key tool for tracing the movement of funds between CASPs.

P2P PAYMENTS AND EXCHANGES: SPECIFIC RISKS AND CONTROLS

3.4. Risks of the P2P Segment and of Centralized and Decentralized Exchanges

Peer-to-peer (P2P) platforms, which allow users to exchange fiat currency for crypto-assets directly without the intermediation of a traditional financial provider, present an elevated AML/CFT risk, since settlement often takes place outside the banking system (cash, transfers through payment apps), and counterparty verification depends on the platform's internal mechanisms, which vary significantly in quality. Typical risks include the use of P2P deals to "cash out" the proceeds of crime, and the recruitment of money mules — individuals who, for a fee, provide their bank accounts or wallets to conduct pass-through transactions.

Centralized exchanges (CEXs), which act as financial intermediaries and control customer assets, are generally subject to direct regulation as CASPs and are required to implement a full set of CDD/EDD, monitoring, and reporting measures. Decentralized exchanges (DEXs) and protocols that operate without a centralized operator, by contrast, create difficulties for applying traditional regulatory tools, since there is no single entity on which to place obligations for user identification — this remains a subject of debate within the implementation of MiCA and the corresponding ESMA guidelines.

An effective control framework at CASP level combines preventive measures (identity verification, screening of counterparty wallets through blockchain analytics tools before crediting/withdrawing funds, limits on transactions with unhosted addresses), ongoing monitoring (detection of patterns characteristic of money mules and pass-through schemes), and staff training to recognize the typical hallmarks of social engineering described above, so that customers can be warned of potential fraud before a transaction is completed.

Building a compliance function that combines the risk-based approach, customer due diligence, and technological monitoring tools is a decisive condition both for protecting virtual asset users from fraud and for CASPs' compliance with EU and Ukrainian regulatory requirements as national legislation is harmonized with the MiCA standards.