

**Banking Supervision Department**

Jerusalem, May 9, 2022

Circular No. C-06-2706

**Attn: The Banking Corporations and Credit Card Companies**

**Re: Management of AML/CFT Risks**  
(Proper Conduct of Banking Business Directive No. 411)

**Introduction**

1. Virtual currencies may be abused for illegitimate purposes including money laundering or terrorism financing, by exploiting the currency's inherent anonymity or via virtual wallets that open without identification of the wallet owner. In this way, cross-border transactions at considerable amounts may be performed without a need for regulated financial intermediaries, in business transactions that are not subject to face-to-face identification, without identity authentication, regulation, or supervision — all of which impede the ability to comply with “Know Your Customer” (KYC) requirements when providing financial services related to customer activity in virtual currencies. As a result, these factors create high potential risk that virtual currencies will be used to perform illegal transactions and used for money laundering and terrorism financing. Still, customer activities in virtual currencies also have the potential to increase the efficiency of international payments and transfers. This position is in line with the positions of the leading international organizations in the field including the Financial Action Task Force (FATF) and the Bank for International Settlement (BIS).
2. At present, regulation and supervision of virtual currency service providers in most countries, including Israel, is still under development. As such, the Banking Supervision Department considers payment services rendered by banking corporations in connection with activity in virtual currency as an activity that carries a high AML/CFT risk and therefore should be subject to increased monitoring and controls. This risk assessment is consistent with the national risk

assessment of the State of Israel in the field of AML<sup>1</sup> that was published in November 2021.

3. In view of the scope of customers' activity in virtual currencies, and consequently the increase in the number of customer requests to transfer funds originating from such activities to payment accounts in the banking system or requests to transfer funds from such accounts for the purpose of activity in virtual currency, I have found it warranted to amend this Directive and to establish unique requirements on the banking system with respect to AML/CFT risk management related to payment services involving customer activity in virtual currency.
4. Completion of the licensing procedure for entities that render financial asset services, including virtual currency services, the entry into force of the "Travel" rule<sup>2</sup> and the establishment of enforcement procedures for implementation of an AML regime by service providers in this field will constitute an added layer in the efforts to reduce the banking system's risk in conducting these activities vis-à-vis service providers in Israel.
5. In view of the above, and after consulting with the Advisory Committee on Banking Business Affairs, and with the approval of the Governor of the Bank of Israel, I amended this Directive.

## **6. Key amendments to the Directive**

Section 87A, "Payment Services Related to Customer Activity in Virtual Currency", will be added in Chapter E of the Directive.

### **6.1 Definitions (Section 87A)**

The following terms were defined: financial asset, virtual currency, virtual currency wallet address, currency, foreign currency, virtual currency service provider, payment services related to customer activity in virtual currency, and virtual currency pathway.

#### Explanatory note:

The definitions for "financial asset", "virtual currency", "virtual currency wallet address", "currency", and "foreign currency" were taken

---

<sup>1</sup> Validation of National Risk Assessment in the Field of AML by the Financial Regulators, November 2021.

<sup>2</sup> The "Travel Rule" requires all financial institutions to pass on, immediately and in a secured manner, certain information to the next financial institution, as stated in Section 7A(b)2 of the AML Order with respect to the activities of credit service providers and financial asset service providers.

from existing provisions of law in Israel and from the Anti-Money Laundering Order that applies to credit service providers and financial asset service providers. It should be emphasized that the definition of a virtual currency in the Anti-Money Laundering Order restricts activities in virtual currency to activities for payment and investment purposes only. For example, “activities in virtual currency” do not include activities in virtual assets that have the features of securities, or activities in a virtual asset that is a digital representation of the value of real estate assets, commodities, works of art, and the like. Furthermore, the terms “payment services related to activities in virtual currency,” “virtual currency service provider,” and “virtual currency pathway” were also defined.

Accordingly, Section 87A of the Directive concerns the receipt of funds originating in activity in virtual currency from accounts of virtual currency service providers to accounts of the banking corporation’s customers who do not engage in such activity exclusively as a business. It is emphasized that all transfers of funds from a customer’s account in a banking corporation to any account of a virtual currency service provider shall be subject to all applicable laws.

## 6.2 **Risk assessment** (Section 87A(a))

The Directive determines that the banking corporation must conduct a periodic assessment on transfers that originate from a source, or are made to a recipient, related to virtual currencies, and must determine a policy and procedures based on the risk assessment and a risk-based approach.

### Explanatory Remarks:

A banking corporation must conduct a periodic risk assessment in the field of activity in virtual currencies, similarly to the other AML/CFT risks that it faces, as stated in Chapter C of the Directive. A specific risk assessment of activities in virtual currencies must be performed in view of the complexity of such activities, their unique features, and their high risk potential. It should be noted that this requirement is consistent with the international standard defined by the FATF on risk-based management of such activity, which calls for a risk-based approach to

such activity and the performance of a risk assessment before executing activities for customers with activity in virtual currencies.

When conducting the risk assessment and developing the policy and procedures, the banking corporation must consider the unique risk factors of activity in virtual currencies, which include but are not limited to customers' anonymity or pseudo-anonymity, the possibility that a business agreement was made without customers' face-to-face identification or authentication, the absence of regulated financial intermediaries in some cases, and the rapid and global nature of virtual currency transfers.

### 6.3 **Policy and procedures** (Section 87A(b))

- (a) The Directive determines that, in the event that the virtual currency service provider that is a party to the transaction is a licensed service provider in Israel, a banking corporation may not refuse to render payment services related to activity in virtual currency only due to the fact that the service is related to virtual currencies.
- (b) The Directive determines that said policy and procedures must address the following issues, at minimum: the mode of operations vis-à-vis various virtual currency service providers, referring to licensed service providers in Israel, service providers that operate under a Continuation Permit, and virtual currency service providers that were incorporated or operate outside Israel; the virtual currency pathways through which the banking corporation permits payment services; the mode of operations vis-à-vis customers who executed activities in virtual currency other than through a virtual currency service provider (P2P).

#### Explanatory Remarks:

The Directive defines several issues that must be included in the policy and procedures to be determined according to the risk assessment performed by the banking corporation and according to a risk-based approach. These issues include but are not limited to: The banking corporation must check the service provider's identity and the AM/CFT requirements that apply to its operations. The Directive determines that

a policy may not include a sweeping refusal in the event of an activity performed through a virtual currency service provider who was granted a license by the Capital Market, Insurance, and Savings Authority to render virtual currency services. Furthermore, the banking corporations are required to set a policy on the activities performed through other virtual currency service providers, in accordance with the findings of their risk assessment. For the sake of clarity, the banking corporations may set a policy not to render payment services related to activity in virtual currency where the service provider does not operate under a license from the Capital Market, Insurance, and Savings Authority, only on the condition that the banking corporation conducted a well-established risk assessment on this matter.

The banking corporations must set a policy on activity through P2P platforms that are performed without the mediation of service providers that are subject to an AML/CFT regime and that, as a result, represent a higher potential risk.

When defining a policy and procedures, banking corporations that issue payment cards must also take into consideration the directives and guidelines of international credit card companies.

**6.4 Source of the funds and the virtual currency pathway (Sections 87A(b)(3-4) and 87A(c))**

The Directive determines that the banking corporation must define the virtual currency pathways for payment services related to activity in virtual currency, and must inquire into the source of the funds used to purchase the virtual currency and the funds' path from the purchase of the virtual currency to the deposit of the funds originating from the sale of the virtual currency in the customer's account with the banking corporation.

Explanatory Remarks:

When determining the virtual currency pathways in which payment services related to activity in virtual currency will be rendered, the banking corporation must take into account pathways that challenge efforts to track the identities of the transferors and transferees. Accordingly, the banking corporation will probably determine stricter

policy and procedures for cases in which the activity in virtual currency includes a conversion or exchange of one or more types of virtual currencies, or activity in which the virtual currencies were transferred through a mixer or other tools that obliterate their transfer route, or activity in which the virtual currencies were transferred between several virtual currency service providers without a reasonable explanation, or activity in a virtual currency that is characterized by a higher degree of anonymity.

Due to the high risk potential entailed in the receipt of funds originating from virtual currencies in the customer's account with the banking corporation, the banking corporation must apply rigorous identification and monitoring procedures including the following: When the customer's activity exceeds the cumulative amount of NIS 100,000 per year, from that amount and onward the banking corporation must also obtain the customer's explanation for the source of the funds used to purchase the virtual currency or finance the mining activities, and for the virtual currency pathway. As necessary, the banking corporation must ask for written documentation that supports said explanation, such as confirmation of the virtual currency pathway from the virtual currency service provider or from another external entity with the appropriate expertise, to the bank's satisfaction. Alternatively, the banking corporation may demand that a virtual currency service provider licensed in Israel provide a certificate of no impediment to perform the transaction. For the sake of clarity, the demand for such confirmations and the identity of the entities providing such confirmations should be defined according to a risk-based approach and according to the bank's acquaintance with the customer, as well as its acquaintance with the amounts of the customer's activity and the complexity of the pathways. Furthermore for the sake of clarity, the above does not detract from all other obligations that apply to the banking corporation with respect to fund transfers.

**6.5 Prohibition on rendering of services in specific cases (Section 87A(d))**

The Directive determines a prohibition on rendering payment services related to activity in virtual currency if, based on the information in the banking corporation's possession, the service provider that is a party to activity in virtual currency is in violation of the laws with respect to licensing or registration requirements in its country of incorporation.

Explanatory Remarks:

According to FATF recommendations, countries must determine registration or licensing requirements for virtual currency service providers. Accordingly, in Israel, the banking corporations are prohibited from rendering payment services related to activity in virtual currency if, based on the information that they possess, the service provider violated the laws related to licensing or registration in its country of incorporation.

**6.6 Disclosure to customers (Section 87A(e))**

A banking corporation shall publish on its website the key points of its policy on payment services related to activity in virtual currency. Furthermore, the banking corporations must inform their customers about their policy on payment services related to activity in virtual currency immediately after the customer's first request to withdraw funds from their account with the banking corporation to an account that is administered by a virtual currency service provider, if the bank identified that the transfer of funds was made from the customer's account with the banking corporation to the customer's account with a virtual currency service provider.

Explanatory Remarks:

Within the banking corporation's relationship with its customers, the banking corporation must inform the customer of its policy on receiving funds in exchange for activity in virtual currency from a virtual currency service provider to customers' accounts at the banking corporation, immediately after and if possible in advance of, the first withdrawal of funds (through any possible channel of activity—through a branch, by telephone, via an app, etc.) from the customer's account at the banking corporation to an account administered by a virtual currency service provider. For the sake of clarity, this requirement applies to the

customer's request to withdraw funds from its account with the banking corporation to its account with any virtual currency service provider, and if the customer operates via several virtual currency service providers, there is no obligation to inform the customer of the bank's policy on this issue at each withdrawal of funds to an account with other virtual currency service providers. Furthermore, the banking corporation must publish on its website the key points of its policy on rendering payment services related to activity in virtual currency.

**6.7 Reporting to the management and board of directors** (Section 87A(f))

At least every six months, the banking corporation must report to the senior management and the board of directors about the scope of payment services rendered in relation to activity in virtual currency, the main risks entailed in such operations, and the manner in which they are being monitored.

Explanatory Remarks:

The reports to the board of directors and the management about AML/CFT-related issues must include reference to the banking corporation's indirect exposure to virtual currencies related to its customers' activities, due to the high potential risk of such activities.

**Commencement**

7. The amendments to this Directive will come into force within six months from the publication date of this Directive.

**Updates**

8. Following are the updates to the Proper Conduct of Banking Business file:

Remove pages	Insert pages
411-1-34 [20] (10/2021)	411-1-36 [21] (5/2022)

Respectfully,

Yair Avidan

Supervisor of Banks