Statement by CTIF-CFI on money laundering and terrorist financing risks related to the use of virtual currencies

As mentioned in the annual report 2016 (as well as the 2017 report) CTIF-CFI closely monitors the issue of virtual currencies and the risk of their use in money laundering and terrorist financing transactions.

Virtual currency exchange platforms are currently not regulated in Belgium. Given that no there is no legal framework for these platforms in Belgium, virtual currency exchange platforms are not subject to supervision or the AML/CFT framework.

CTIF-CFI consequently does not receive any disclosures from exchange platforms in Belgium.

Nevertheless, credit institutions in Belgium could be faced with atypical transactions related to virtual currencies and inform CTIF-CFI of these transactions. As part of international information exchange with foreign financial intelligence units in countries in which virtual currency exchange platforms are regulated, such as Luxembourg for example, CTIF-CFI may also receive spontaneous information on suspicious transactions involving virtual currencies as a result of a disclosure by a foreign platform for exchanging virtual currencies. This information is subsequently processed like a disclosure.

The transactions with virtual currencies in these files are mostly international payments from or to these exchange platforms with accounts abroad. It should be noted that numerous persons first use a payment service provider before sending the funds to an exchange platform. In some cases these exchange platforms are located abroad, making it difficult to obtain information on the origin or the destination of the funds. CTIF-CFI's investigation is hampered by the fact that these payment service providers are used and act as an intermediary.

The virtual currency exchange platforms are not only used to change virtual currencies into legal tender and vice versa, but also to convert virtual currencies into other virtual currencies that can be used more anonymously such as *monero* or *dash*[1].

CTIF-CFI received information on illegal exchangers who change virtual currencies into cash (or vice versa)[2]. These services are provided by online service providers, for large amounts and for a commission that is much higher than the usual fee to be paid using the common channels of online exchangers. Police information indicated that, after a first contact through the exchange platform, secure communications are used to establish the terms of the transaction. The physical transfer then takes place during brief encounters with customers in public places. Although it may seem that exchange transactions of "dirty" cryptocurrency for cash using these online service providers could go unpunished, criminal proceedings show that these illegal online services are not as anonymous as these service providers and their customers might think. One recent example is the takedown of the illegal online marketplaces *Alphabay* and *Hansa* as part of criminal investigations abroad[3].

[1] Europol, 2017 Virtual Currencies Money laundering Typologies, Targeting Exchanges and other CyberGatekeepers, The Hague, 31/12/2017.
[2] *De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten* [The bitcoin trader, a facilitating role with cash-out of criminal proceeds], Anti Money Laundering Centre, August 2017, De Bilt.
[3] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

In 2016 and 2017, CTIF-CFI processed disclosures received from credit institutions on suspicious or atypical financial transactions with platforms for exchanging virtual currencies located abroad.

The transactions of these disclosures have the following characteristics:

- receipt of transfers from virtual currency exchange platforms, followed by cash withdrawals;
- numerous cash deposits followed by the purchasing of virtual currencies on exchange platforms;
- intensive use of payment service providers for transactions via virtual currency exchange platforms;
- conducting non-official trader activities in virtual currencies without declaring these activities to the tax authorities. The transactions consist of numerous domestic and international transfers from many different counterparties and cash deposits, followed by buying and selling virtual currencies via exchange platforms for third parties.
- the transactions on the bank account are not in keeping with the known profile of the customer, who does not carry out any declared activity, who carries out declared activities related to suspicious transactions or to transactions seemingly carried out for third parties.
- the customer uses exchange platforms known to facilitate the anonymous change of virtual currencies into cash and vice versa (*LocalBitcoin* for example).

It should be noted that, depending on the circumstances, it may be compulsory to declare the income / added-value from buying and selling virtual currencies.

Virtual currencies can be used for money laundering or terrorist financing purposes but also to commit fraud. Fraud usually relates to investments in cryptocurrencies. These files have the following features:

- transfers with investments in cryptocurrencies as a justification, for which the customers mentions an disproportionate return;
- receipt of multiple transfers of large amounts on an account held by a private individual / foreign company without any known activity in Belgium, with reference to investments in cryptocurrencies;
- receipt of transfers of large amounts followed by transfers to financial centres susceptible to money laundering where funds can disappear more easily.

Often these files are brought to light following complaints from customers about investments in cryptocurrencies. On its website the FSMA publishes a list with suspicious websites offering fraudulent trading transactions in cryptocurrencies. The FPS Economy and the FSMA developed a website that can be used to check whether a website is unfavourably known (https://tropbeaupouretrevrai.be/trop-beau-pour-etre-vrai).

CTIF-CFI also took part in a study on virtual currencies led by the Canadian FIU FINTRAC.

This study shows that bitcoin is the most frequently used virtual currency for illegal activities, in addition to other virtual currencies such as *Ethereum*, *Dogecoin* and *Litecoin*. In most jurisdictions the number of disclosures of suspicious transactions related to the use of bitcoin rose in the past three years.

Even though the blockchain technology facilitates finding and tracing virtual currencies, the traceability of transactions is one of the main problems identified by financial intelligence units that took part in the project. The identified difficulties mainly relate to the use of technologies through which the identity of people using or carrying out transactions in virtual currencies can be concealed. These technologies make it possible to hamper the identification of an IP address or mix several transactions using virtual currencies.

The lack of a legal framework regulating virtual currencies, virtual currency exchange platforms and custodial wallet providers in many jurisdictions increases money laundering or terrorist financing risks. Due to the lack of a legal framework some platforms or persons can carry out the activity of exchanging virtual currencies without having to request a licence or apply AML/CFT measures.

Many jurisdictions recorded a sharp rise in the number of BTMs, such as BTMs installed in casinos and arcades. BTMs can be used to change cash into virtual currencies without extensive identification procedures, or vice versa, virtual currencies into cash. BTMs generally accept bitcoins as well as other cryptocurrencies such as *Ethereum*, *Litecoin*, *Dash*, *Bitcoin Cash*, *Dogecoin*, *Zcash* and *Monero*.

In some jurisdictions it was established that BTMs were used by criminal organisations to launder money of illegal origin. Once the cash was changed into bitcoins the bitcoins can easily be moved to another jurisdiction and potentially withdrawn in cash via a BTM in this other jurisdiction. In Belgium there is no legal framework regulating the installation and the use of these BTMs.

A number of indicators of suspicious transactions identified at national level were also identified at international level:

- a large number of transfers from third parties, followed by transfers to virtual currency exchange platforms;
- selling virtual currencies, immediately followed by cash withdrawals;
- the customer provides financial services (virtual currency exchange platforms) without having the required licence;
- the customer cannot demonstrate that he has fulfilled all of his fiscal obligations although he seemingly regularly exchanges virtual currencies (exchange platforms);
- the customer provides vague or inconsistent explanations on the origin of the funds;
- there is no economic rationale behind the transactions;
- the transactions are not in keeping with the customer's profile;
- rounded amounts are transferred to a bank account, followed by transfers to virtual currency exchange platforms. This can be explained by the fact that the customer and account holder is an intermediary who launders proceeds of crime for a criminal organisation;
- virtual currency transactions are conducted through virtual currency exchange platforms located in jurisdictions with no or little supervision on exchange platforms;
- repeated transfers without any justification of funds from companies operating BTMs (to change cash into virtual currencies);
- the customer uses over-the-counter platforms to change virtual currencies, these platforms facilitate anonymous exchange transactions between private individuals, sometimes in exchange for cash and vice versa (*LocalBitcoin* for example);
- the documents presented by the customer to justify his investment in cryptocurrencies are of bad quality, incomplete, fraudulent or contain little information on the investment proposal.

Finally mention should be made of the risks of TBML practices in combination with the use of virtual currencies. According to a report by the Drug Enforcement Administration[4] many China-based firms manufacturing goods used in TBML schemes now prefer to accept Bitcoin. Bitcoin is widely popular in China because it can be used to anonymously transfer value overseas, circumventing China's capital controls.

[4] DEA. 2017 National Drug Threat assessment, page 130. Accessed online on 13 December 2017: https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf