# Crypto exchange providers

## - Professional Money Launderers

Information classification Open

Swedish Police Authority, Financial Intelligence Unit, September 2024

Publisher: Swedish Police Authority, National Operations Department, Financial Intelligence Unit, 106 75 Stockholm
Ref. No.: A554.682/2024 – 423
Cover photo: Mostphotos
Edition: Intrapolis
Date: 23 September 2024

## Summary

Based on the analysis by FIU Sweden, illicit crypto exchange providers are predominately individuals that provides unlicensed and illegal services to convert criminal proceedings into cryptocurrencies, or the other way around, cryptocurrency earned from crime into cash or other forms of assets. Criminal proceedings from all types of crimes can be laundered via cryptocurrency, and the crypto exchange provider is often a sought-after expertise within the criminal economy, usually operating with an international reach.

Based on their specific characteristics, the crypto exchange providers fit the role of a professional money launderer (PML)[1]. In order to provide a deeper understanding of how these perpetrators operate, FIU Sweden have identified four main profiles of crypto exchange providers with a number of underlying characteristics, that are presented in the report.

FIU Sweden assesses illicit crypto currency providers as an emerging threat within money laundering and other severe crimes, and are considered to play a crucial role for the expansion of organized crime. Therefore, a range of measures involving supervision, monitoring and law enforcement are outlined. One important conclusion is that measures targeting PMLs, such as crypto exchange providers, tend to have a greater impact than measures against criminals that solely conduct their own money laundering, as they often provide their services to more than one person. If such functions are disrupted, the stability of their entire criminal system can be affected.


[1] A PML can be described as a person who systematically launders money for others in return for payment.

# Table of contents

**Summary** ..... **3**

**Table of contents** ..... **4**

**1 Introduction** ..... **5**

**2 Crypto assets in money laundering** ..... **6**

**3 Illicit crypto exchange providers** ..... **7**

3.1 Professional Money Launderers ..... 8

**4 Information status** ..... **9**

4.1 Modus operandi ..... 9

4.2 Subgroups and characteristics ..... 10

**5 Example cases - Links to criminal networks** ..... **11**

**6 Assessment** ..... **12**

6.1 Law enforcement, supervision and monitoring ..... 12

# 1 Introduction

This report is produced by FIU Sweden in order to outline the fundamental analysis and conclusions brought out of a previous in-depth intelligence report about illicit crypto exchange providers. The crypto exchange providers described in this report are individuals who offer services in crypto exchange, sometimes referred to as illegal crypto exchange providers, underground banking, black-market exchange providers, private exchange providers or virtual crypto exchange providers.

With this report we are now providing open access to essential assessments and arguments in order to explain the increasingly high risks involved within the field of crypto exchange operations. In addition, we are also presenting guidance and recommendations concerning relevant authorities as well as obliged reporting entities, both in Sweden and internationally, to combat these highly specialized money laundering offenders with close ties to organized crime.

# 2 Crypto assets in money laundering

Cryptocurrencies are increasingly used in the context of money laundering.[2] As the use of cryptocurrencies has become more widespread in general, both as an asset and as a payment method, the increase in attractiveness also appears to be present within many parts of the criminal arena, and the transaction volumes in crypto assets may seem limitless in some crime areas. This increase is also shown by the number of submitted suspicious transaction reports (STR) to FIU Sweden regarding crypto assets.[3] The possibility to launder large volumes of assets between crypto wallets internationally, without involvement of a third-party operator, and not necessarily exposing your own identity has drawn attention to the crypto world, specifically for transactions with criminal intent. There are various international estimates of the illicit volumes as part of the crypto economy in total, these estimates vary from less than one percent to closer to a quarter of the total crypto volumes.[4] However, it can be argued that substantial volumes of the international crypto flows are mainly upheld by criminal activities. Some intelligence data gathered by FIU Sweden provides support to assume this.

Criminal proceedings from all types of crimes, both “traditional” crimes and in the cybercrime arena, can be laundered by the use of cryptocurrency. Furthermore, new tools and methods to mask and hide the criminal traces are being designed and perfected.[5] Even though crypto assets are traceable to a large extent, there are solutions solely provided to mask criminal identities and transactions with criminal origin, and by that hinder actions taken by authorities and obliged reporting entities. A variety of crypto mixers and swappers, many of which are illegal, are frequently occurring in the blockchains.

The use of crypto assets in a criminal context is often closely associated with activities on the cyber domain, often the darknet. According to data analyzed by FIU Sweden, an increasing proportion of some criminal markets are occurring on the cyber domain, i.e. drug dealing, illegal streaming services, various frauds and sadly also sexual abuse material, just to mention some. In turn, many of these illicit activities generate substantial amounts in cryptocurrency payments. The proceedings may then be laundered in a series of schemes domestically and internationally, not only via crypto but a variety of other assets. In addition to this, the use of crypto assets is an established method for sanction evasion and also terrorist financing.

---

[2] EU SOCTA 2021 - Serious and Organised Crime Threat Assessment. A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime. Europol, 2021.

[3] Penningtvätt och finansiering av terrorism med kryptovalutor, Polismyndigheten, november 2022

[4] Ibid

[5] Ibid

# 3 Illicit crypto exchange providers

A crypto exchange provider is an individual that often possesses a sought-after expertise within the criminal economy, and functions as an enabler. This is done by providing unlicensed and illegal services to convert criminal proceedings into cryptocurrencies, or the other way around, cryptocurrency is exchanged into other forms of assets.

The role of the crypto exchange provider can be wide and multifaceted, and is often a critical part in money laundering schemes involving crypto assets. The actual trade is often managed through physical meetings with the illicit customer when payment is done by cash, or remotely if the trade is done via digital payment. According to intelligence gathered by FIU Sweden the predominant way of trading is between cash and crypto, but the use of instant payment transactions, bank accounts and luxury goods are also existent in various levels. The crypto exchange provider may use legitimate crypto platform accounts to acquire the cryptocurrency. When transferring the cryptocurrency to the criminal, private crypto wallets are often utilized.

These individuals can be described as a form of “money broker”, specialized in enabling crypto transactions. It can also be stated that some crypto exchange providers play the role of a middle man, providing assets in both directions, supplying criminals with different financial needs. Some of the individuals provide their services widely, sometimes also for legit purposes, but are often highly neglectant to the fact that they enable money laundering and other severe crimes. Such activities may then make up the reason for a suspected commercial money laundering felony.

Trading cryptocurrencies via an established and legitimate crypto trading platform, is often easier, safer and cheaper for any legitimate consumer. But the reason for criminals to instead turn to an illicit and unlicensed crypto exchange provider can be the need for anonymity, avoidance of controls, lack of know-how, or the need to exchange between cash and cryptocurrency. Criminals may set aside several percent of their assets in fees to the crypto exchange provider. Given that cryptocurrency trading currently is very easily accessible through regulated and legitimate marketplaces, it is questionable whether there is a need for the services of crypto exchange providers other than for criminal schemes, such as money laundering.

## 3.1 Professional Money Launderers

Based on the characteristics described above, the crypto exchange providers fit the role of a professional money launderer (PML). A PML[6] is usually described as a person who systematically launders money for others in return for payment. In the context of this report, a PML is referred to as crypto exchange provider, who offer services in crypto exchange on behalf of criminals.

FIU Sweden has recently published a report describing the context and extent of PMLs.[7] What distinguishes the PMLs is that they may have access to different types of systems, or have specific powers through their professional role, which makes it easier for criminals to launder money or otherwise manage their criminal proceeds. Others are not professionally qualified but have specialized skills that are in high demand, which is applicable to individuals offering crypto exchange services on behalf of criminals. While PMLs are sometimes linked to specific criminal networks, they generally appear to serve several different individuals and criminal networks. This is in line with the trend towards more mobile network structures: money laundering and other criminal schemes are bought as a service.

PMLs may act individually based on their specific expertise or cooperate with each other to offer more services. There are also entire PML organizations with established money laundering concepts with a clear division of roles within the organization, such as hawala- and underground banking networks. Some PMLs are multidisciplinary and have an entire group consisting of several companies and utilize other PMLs in various industries. All this may also be found within the investigation of an illicit crypto exchange provider.

All in all, the assessment from FIU Sweden is that there is an increasing demand for PML from organized crime and that the services they provide are pivotal for the criminal economy. PMLs within some segments of the crypto area can be easily accessible for criminal networks, but the access to specialized expertise is sought-after but limited. This is underlined by the dynamics of many PMLs that have been identified by the FIU. The characteristics of different subgroups of crypto exchange providers are further outlined in this report.

---

[6] Abbreviation for Professional Money Launderer. The term was developed by the inter-governmental body FATF.

[7] Professional Money Launderers, lndustries, modus operandi and links to criminal networks, Swedish Police Authority, Financial lntelligence Unit, August 2024

# 4 Information status

The ability to detect information about crypto exchange providers has proven to be greater than for many other PMLs based on FIU Sweden's analysis and operational work. This is because some crypto exchange providers relatively often offer their services publicly on what are known as peer-to-peer cryptocurrency platforms[8], in online forums and in chat rooms. In this way the trade is partly transparent, thus criminals can sometimes be identified. However, these perpetrators are not licensed by the Financial Supervisory Authority (FSA)[9], as they are required to. This limits the information available to the Swedish Police Authority and other agencies. There are also individual crypto exchange providers that are more tightly connected to criminal networks, who do not typically advertise their services publicly.

## 4.1 Modus operandi

Some crypto exchange providers have deep knowledge of cryptocurrencies and thus the capacity to enable, in addition to crypto exchange, advanced money laundering and cryptocurrency management in criminal schemes.

The initial contact between currency-exchange providers and customers typically takes place in dedicated forums, in chat groups or on the peer-to-peer crypto trading platforms mentioned above. Two methods of cryptocurrency exchange for cash and digital payment methods are described below.

- **Currency exchange by cash payment.** In a cash/crypto exchange operation, a physical meeting takes place, the crypto-transaction is carried out and cash is handed over. In some cases, the crypto wallet is controlled by a third person remotely and so the transaction needs to be confirmed by sending a screenshot. The recipient of the cryptocurrency, which is usually in bitcoin, then sometimes converts it into a 'stablecoin'[10] to avoid price fluctuations.

- **Currency exchange through digital payment methods.** In digital payment exchange operations, crypto exchange providers and customers find each other on, for example, peer-to-peer platforms, where the terms of the transaction are discussed. Money is sent digitally, e.g. via the mobile payment system Swish (Instant payment), and the cryptocurrency is transferred between the parties' crypto wallets. Both parties confirm when the transaction is complete. However, it should be emphasized that crypto exchange through digital payments can also be handled entirely outside peer-to-peer platforms.

---

[8] Peer-to-peer (p2p) platforms offer sale of cryptocurrencies directly between users. Users can create adverts to buy or sell cryptocurrencies and conduct transactions with other users.
[9] Finansinspektionen

[10] Stablecoins are a type of crypto-asset that are intended to maintain a stable value over time, for example by tracking the price of a national currency such as the US dollar.

## 4.2 Subgroups and characteristics

Based on this analysis, FIU Sweden have identified what we see as four main profiles of crypto exchange providers, i.e. subgroups. These are distinguished by a number of underlying characteristics, see below. The subgroups are set up in order to gain a deeper understanding on how these perpetrators operate, their magnitude, their criminal range, and who their criminal client base is. In turn, this can provide guidance to what measures are most suitable to combat the different subgroups.

### The Node Exchange Provider

- Plays a significant role in the criminal economy - Integrated into criminal networks
- Relies on criminal connections to manage trades
- Low number of perpetrators – sought after expertise and hard to replace in the criminal arena
- Trades in both directions (cash/crypto mainly)
- Access to couriers, front men, cash, cryptocurrencies via connections

### The Hawala Exchange Provider

- Connected to hawala/underground banking networks
- Wide spread international connections
- Exposure to the middle east
- Access to couriers, front men, cash via network/diaspora
- Often operating based on the network's origin
- Occur in dedicated social media forums (specifically hawala/money transfer)

### The Asset Exchange Provider

- Part of an illicit business with a systematic use of crypto assets
- High capacity to trade crypto in volume
- Usually trades crypto for own needs
- Often able to provide services cheaper or even at a loss
- Low number of perpetrators in the market

### The Platform Exchange Provider

- Advertising their intention to trade on open P2P platforms and crypto forums
- Selling exceeds buying
- Accepting payment with instant transfer, cash or bank account
- Less likely to be linked to organized crime
- Servicing small-scale narcotic buyers and fraud offenders
- Large number of perpetrators in the market

# 5 Example cases - Links to criminal networks

Crypto exchange providers in the form of PMLs can accommodate a diverse client base, for example some clients need to exchange cash to crypto and some need to convert crypto back to cash. They operate both within criminal networks (may serv other criminal networks simultaneously), or as independent providers with different types of clients. Below are two separate examples of perpetrators who were convicted of, among other things, money laundering- and commercial money laundering offences, through crypto exchange on behalf of various clients, in 2022[11] respectively 2024.[12]

The description of the first offence shows that the individual:

*"between 27 March 2020 and 1 June 2021, acting together and in collusion with others in various places in Europe and in the municipality of Uppsala, Sweden, received, stored and traded cash and cryptocurrency amounting to at least SEK 30,269,175 (approx. EUR 3M) in return for payment in order to conceal the fact that the money derives from criminal activity. In so doing, [the individual] illicitly promoted the possibility of another person appropriating the property. (...) The offence is to be assessed as gross due to the large values handled and to the fact that the measures were part of large-scale criminal activities that were difficult to detect."*

The prosecutor stated that the individual had received, stored and traded the cash or cryptocurrency for a fee. As regards the cryptocurrency, this had been done via crypto wallet to which the individual had direct or indirect access on behalf of various clients.

In the second example, one of the convicted felons was concluded to have taken part in illegal hawala transactions by operating as a crypto exchange provider:

*"The crypto currency exchange operations were an independent part of [the individual´s] activities who partly financed themselves by [the individual] using cryptocurrency to buy cash and then to buy new cryptocurrency. [The individual] was part of a network of financial intermediaries. For example, one money intermediary had a customer who wanted to send money to Sweden, and another money intermediary had a customer who wanted to send money to Iran, and the amount was then settled in whole or in part against each other."*

The prosecutor alleged that [the individual´s] activities involved crypto currency transactions of at least SEK 74 million (approx. EUR 7,4M). In addition, account statements from [the individual´s] bank has shown that a large amount of instant payments was labelled "hawala".

[11] Uppsala District Court judgment 2022-11-23 - B 4490-21. The person was also convicted of exceptionally gross narcotics offence and gross narcotics offence.

[12] Attunda District Court judgement 2024-04-23 - B 13832-23.

# 6 Assessment

The demand for crypto exchange services is very high among criminals, which suggests that the use of cryptocurrency is widespread within the criminal arena. This is particularly evident in areas such as drug crime and fraud in the cyber arena. It can also be concluded that these types of illicit crypto services have a wide spread international scope, with obvious cross-border capacities. By fueling the criminal infrastructure, the crypto exchange provider is part of a larger context. Their services support influential criminals in organized crime, thus helping to finance the spiral of violence and other serious crime.

Some of these crypto exchange providers operate in the periphery, seemingly separate from other criminal arenas of organized crime, and can therefore be difficult to detect for both regulatory and law enforcement agencies. But there is also a significant number of Swedish users of individual crypto exchange providers who mainly operate relatively open on peer-to-peer platforms. The range in turnover is wide, sometimes with a large number of transactions and significant values. Some individual crypto exchange providers cannot always be classified as PMLs due to not necessarily having a criminal intent, but as a group they play an important part as enablers for the criminal economy anyway. To conclude, FIU Sweden assesses illicit cryptocurrency providers as an emerging threat within money laundering schemes and a crucial part for organized crime to maintain and expand their criminal markets.

## 6.1 Law enforcement, supervision and monitoring

Law enforcement must steadily increase its presence on different platforms used for crypto exchange in order to identify and map illicit crypto exchange providers. Since the entire crypto arena has an international scope, it must be a necessity for law enforcement agencies to conduct joint international operations, involving agencies in- and outside the EU, in order to share vital data and gain important synergies. In general, measures targeting PMLs tend to have a greater impact than measures against criminals that solely conduct their own money laundering, as PMLs often provide their services to more than one person. This is therefore truly valid when it comes to crypto exchange providers. If such functions are disrupted, the stability of their entire system can be affected or even eliminated.

Further, the illicit crypto exchange providers are engaged in such business activities that requires registration with the Swedish FSA and to comply with the AML legislation, which they are not- and do not do. In addition, the FSA's ability to sanction unlicensed crypto exchange providers has been limited so far, thus it needs to be strengthened. Such business activities may also be subject to other crimes such as tax offences and accounting violations.

Obliged entities such as banks, neobanks and payment service providers also play a crucial role here. Entities must have sufficient monitoring in place to detect accounts with deviant transaction patterns in- and out of crypto trading platforms, as well as suspicious transfers from other account holders. Also, excessive amounts of instant payments (such as Swish transactions) can call for deeper investigations and further actions by the reporting entities. Dubious users need to be identified and investigated, and the possibility to continue their activities needs to be stopped, for example by restricting their access to services. Suspicious transactions and activities must be reported to the FIU.

Moreover, licensed and legitimate crypto trading platforms need to be very observant of any deviant patterns of trading on their client's wallets, and on that basis take necessary actions with regards to the AML legislation requirements. This could lead to stopped transactions and offboarding of dubious clients. As with all obliged entities, suspicious transactions and activities must be reported to the FIU.