Regulating Crypto: The 5th AML Directive

Tassos Repakis, ESQ., L.LM.

Head of Legal & Compliance, CoinSchedule; Of Counsel, Andersen Legal

Some Background

- AMLDs are a by-product of *FATF* recommendations
- AMLD1 (1991); AMLD2 (2001);
- AMLD3 (2005) included measures against terrorism financing for the first time
- In 2015 the existing framework was substantially revised by AMLD4 & FTR
- AMLD5 (2018) expands to crypto-assets – defines “virtual currencies”
- Implementation of AMLD5 provisions by January 10th, 2020

What is Cryptocurrency?

Crypto-assets are a type of private asset that depends primarily on cryptography and DLT. Examples of crypto-assets range from cryptocurrencies or virtual currencies, like Bitcoin, to digital tokens issued through ICOs. Some crypto-assets have attached profit or governance rights (i.e. Security Tokens) while others provide some consumption value (i.e. Utility Tokens). Still others are meant to be used as a means of exchange. Many have hybrid features. Crypto-assets are relatively new and the market is evolving. According to CoinMarketCap, there are **2890** cryptoassets outstanding, with an approx. market capitalization of **$263B**.

“Virtual Currencies”

The “all inclusive” definition by AMLD5:

“a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically”

AML challenges posed by Virtual Currencies

- The “anonymity” of virtual currencies allows their potential misuse for criminal purposes.
- AML regime prior to AMLD5 did not cover service providers in the crypto-sphere (i.e. wallets, crypto-exchanges, etc.), so cryptocurrencies appeared to be unregulated.
- Even in AMLD5’s preamble, it is acknowledged that the measures introduced are insufficient, as crypto-holders can also transact without using service providers within the AMLD5’s regulatory perimeter (i.e. “obliged entities”).

Scope of AMLD5 on Crypto Service Providers

- Exchanges of “virtual currencies” and custodian wallet service providers are now “obliged entities”.
- This means that AMLD4 obligations that apply to financial institutions shall also apply to them too.
- In simple words, crypto-exchanges and wallets shall need to perform CDD and submit SARs.
- MSs shall ensure that crypto-to-fiat exchanges, and custodian wallet providers, are registered with the local regulator.
- FIUs are given the mandate to obtain the addresses and identities of owners of virtual currency – and so push back against the anonymity associated with the use of crypto

AMLD4 & FTR deficiencies

AMLD4 + FTR

- transfers accompanied by the name, account number, address, official personal document number, customer ID or DOB & POB, payee name account number
- Absence of the above trigger SAR to FIU.
- The above apply to transfers of “funds”; crypto does not fit the definition, so out of scope.
- Falls under definition of “property”, as cryptoassets could be “incorporeal immovable assets”.
- However, exchange and wallet service providers are not included in the list of ”obliged entities”, so still out of scope

AMLD5

- Crypto-exchanges and wallets are now “obliged entities”
- CDD/SAR obligations apply
- As “obliged entities” they must be registered centrally
- FIUs can obtain addresses and ID info of persons owning crypto

Potential AMLD5 deficiencies

- Crypto-mining not covered: although mining is technical in nature, miners are users of virtual currencies themselves, thus making the mining business susceptible to illegitimate use.
- AMLD5 covers only crypto-to-fiat exchanges, and not crypto-to-crypto exchanges.
- P2P exchanges (or DEXs) are also out of scope, and are hard to include within the scope as they are operated by software (usually open-sourced), and not entities.
- Only custodian wallet providers that take (online) custody of customer's keys are "obliged entities" – not hardware & software wallet providers, as they do not safeguard keys on behalf of their customers.
- Initial Coin Offerings or equivalent token crowdsales or airdrops are also out of scope.

Some Insights

How “anomymous” is a cryptocurrency like BTC?

Contrary to popular belief, BTC is not, strictly speaking, anonymous. In fact, it’s pseudonymous; your identity is tied to publicly available pseudonym. This pseudonym is a long string of numbers which acts as your bitcoin address. In addition, as the transactions are stored on a “public ledger”, anyone can readily see the records of all of the transactions that have ever involved your bitcoin address. In simple words, you remain “anonymous” until someone connects your publicly available pseudonym to your real world identity.

Some Insights (Cont'd)

- The estimated amount of **money laundered globally** in one **year** is between $800 billion - $2 trillion in current US dollars. This corresponds to approx. 2 - 5% of **global** GDP.
- This is up to 6.5x the total crypto market cap.
- While in the absence of regulation to-date, research also indicates that for every $1 that's being laundered using bitcoin, there's $800 being washed through fiat.
- None of the above should be interpreted as an argument against regulation, but it is important to 'cut through the noise' in order to protect and promote innovation.
- Don't assume - do your own research.

Thank You for Your Attention!
Happy to Take Your Questions