Cryptocurrencies - Risk Assessment & Source of Funds/Wealth Considerations in the context of Conveyancing Transactions

Background and Scope

The Law Society of Scotland (LSS) anticipates that the volume of clients wishing to use funding which derives or has derived from cryptocurrency (crypto) will increase over the coming years.

Using a source of funds that derives from crypto is entirely legitimate, however it remains inherently high risk and the profession should consider the following information to support potential enhanced due diligence requirements across such matters.

The decision to act for a client whose funds derive from crypto should be considered and documented in detail within the client/matter risk assessment and in the context of the practices risk appetite. The practice should have in place appropriate controls to mitigate any risks present and document these accordingly.

Overarching crypto risks include:

- Pseudo anonymity, particularly where anonymised coins or mixers/tumblers are used (see below)

- Its continued use in underlying/predicate crimes, e.g., it's use on the dark web including for the purchase of illegal drugs, arms and weapons and certain types of consumer investment frauds such as Ponzi schemes.

- Crypto remains unstable and highly volatile

This advisory note is in respect of whole or partial private funding of conveyancing purchases where this funding has already been converted from crypto to fiat currency *(i.e., a government-issued currency that is not backed by a physical commodity, such as gold or silver, but by a government).*

It does not extend to situations where a client wishes to fund a transaction directly (either wholly or partially) using cryptocurrency.

What is "crypto"?

The Financial Action Task Force (FATF) defines a virtual asset as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies.

The term Cryptocurrency - or crypto - relates to the concept that digital assets may be designed to be used as a method of unconventional payment and are a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

There are many crypto assets, and you may have heard of some tokens in the news, such as Bitcoin and Ethereum.

A cryptocurrency exchange is an online platform that allows customers to trade cryptocurrencies – either in exchange for conventional fiat money or for other cryptocurrencies.

Assessing the AML risk associated with crypto currencies/assets

A client's involvement with crypto may not in itself present immediate AML/TF concerns, however, the use of crypto is a higher risk factor to be considered during risk assessment (as per LSAG Guidance s 5.6.1.3).

As a result, Practices should strongly consider Enhanced Due Diligence (EDD) measures when sources of funds/wealth are derived from or via crypto.

Practices should consider/document the following:

- Is this within my practice risk appetite?

- Is the use of crypto in keeping with my knowledge of the client, their background and the context of the client/matter? Does the rationale for the use of crypto make sense?

- What is the value of the deposit coming from crypto? How did that asset perform and over what period? i.e., has the asset grown or fallen in value? Can your client provide evidence of this from their crypto account?

- Can you establish and evidence how the client funded the original acquisition of the cryptocurrency (i.e., their original source of funds/wealth). Is the explanation in line with your knowledge of the client, and can this be evidenced?

- Can the client provide evidence of the crypto portfolio? Such as:
    - When was it created?
    - Evidence of deposits from the client?

- Consideration should be given to whether the crypto wallet is hosted or unhosted. A crypto wallet can be software or hardware that allows users to store and use crypto. Unhosted wallets are a type of self-custody wallet that allow users to keep their balances off an exchange.

  If unhosted, can the client prove they have control of the wallet? Consideration should be given as to how the practice would gain comfort around this. i.e., can the client provide screenshots of the wallet, or send a trivial amount to/from the wallet to prove ownership? (commonly known as the "Satoshi Test")

- Do you have access to any specialist reports (often called Blockchain analytic scans) which provide an understanding of the provenance of the funds used? Can the client provide these?

  There are a number of companies that can provide these services, supporting AML compliance in this area. While the LSS does not recommend an individual company, a simple internet search of “*blockchain analysis companies”* will return various providers.

- Has the client used a reputable crypto service provider? Is it regulated by the FCA? (Some wallet providers remain unregulated and/or are based outside the UK).

  A list of the regulated firms can be found here. Regulated crypto businesses are subject to the MLR’s and are supervised for AML purposes by the FCA (see below section re. the UK regulation of crypto).

- Red flag: has the client used a mixer/tumbler service? (see below). The client should be able to provide evidence that such as service has not been used by showing the end-to-end journey of the crypto through their wallet.

High Risk Mixer/Tumbler Services

Mixer (tumbler) services are a way for a person to gain a level of anonymity while making crypto transactions. This service allows for potentially identifiable funds to be mixed with others in an attempt to disguise the trail.

Should it become apparent that a client has engaged in this type of transaction (or cannot show the end-to-end journey of the crypto through their wallet) this should be taken as an inherent red flag, and robust enhanced due diligence measures applied, including seeking a reasonable explanation from the client as to why they have used such a service.

Mixing services are not supported in the UK, therefore consideration should also be given to any geographical risks inherent in the jurisdiction in which this activity has occurred including whether the same level or standard of AML regulation is applied within this jurisdiction.

The LSS regards the use of crypto mixers/tumblers as an inherently high-risk factor/red flag.

UK Regulation of Crypto

Since 10 January 2020, all UK crypto service providers have been in-scope of the Money Laundering Regulations 2017, must be registered with the Financial Conduct Authority (FCA) and are regulated for AML purposes. Further information on this can be found:

- Money Laundering Regulations 2017, as amended
- Cryptoassets - FCA

LSAG 5.6.1.3 states “where an entity is supervised for AML itself (high value goods businesses, crypto-asset wallet providers etc.) to a comparable standard, this may be seen as presenting reduced risk”. Such factors should be considered within the individual client/matter risk assessment undertaken.

Summary

Fundamentally, many customer due diligence considerations in relation to source of funds and source of wealth remain the same no matter whether crypto assets have been used or not.

There is no one-size-fits-all when it comes to applying risk-based, robust and holistic due diligence.

That said, when the source of funds/wealth to a transaction involves the use of crypto, there are a number of additional considerations to be documented in any risk assessment performed, as outlined across this advisory note.

These should be considered, clearly articulated and recorded across the risk assessment and due diligence performed.

Please be aware that any such transactions undertaken must also be disclosed as part of the next AML Certificate submission.

Suspicious Activity Reporting

As always, if you know or suspect a person is engaged in money laundering or dealing with criminal property you must submit a suspicious activity report to the National Crime Agency (NCA) through the NCA SAR online portal. The NCA glossary code used in relation to concerns around crypto is XXVAXX and should be used accordingly.

Further Information:

Further information can be found at:

FCA Guidance
JMLSG Guidance (Pt II, Chapter 22)
LSAG Guidance
FATF Guidance