ICAEW KNOW-HOW
INTEGRITY AND MARKETS

CRYPTO-ASSETS: ANTI-MONEY LAUNDERING GUIDANCE FOR ACCOUNTANTS

GUIDE

CONTENTS

INTRODUCTION

The world of crypto-assets can sometimes appear veiled in hype and horror stories and impenetrable “tech-speak”. This guidance is designed to be read by accountants before they undertake their first assignment for a client associated with crypto-assets. It will also be a useful resource for accountants undertaking subsequent assignments for such clients.

Part three of this guidance explains the basics of crypto-currencies and the terminology used to describe them. Part four discusses when you may encounter customers in the crypto-asset market. Part five discusses the relevant money laundering risks, and parts six and seven considers how to mitigate these risks.

WHY THIS MATTERS TO YOU

Individuals engaged in criminal activity often seek the services of unwitting professional advisers such as accountants to hide criminal activity from law enforcement, and add a facade of legitimacy to the proceeds of crime.

Crypto-assets offer a novel solution for individuals looking to engage in criminal activity. Illicit goods and services are now traded internationally on the ‘dark web’ in exchange for crypto-assets. In some circumstances, crypto-assets can offer far greater opacity than traditional fiat currencies (such as GBP, USD and CNY), making it more difficult to trace the proceeds of crime.

With business models exploiting this new form of wealth transfer, accountants need to turn a critical eye to how this economic activity is recorded. You should seek to understand how to reconcile existing accounting and finance concepts with new value transactions; equally you should seek to understand how growth in new financial technologies brings with it a potential corresponding increase in ways to evade the law. Consequently, it pays dividends to familiarise

yourselves with crypto-assets if only to ensure that we protect ourselves and our clients against risks, while capitalising on the rewards.

THE BASICS OF CRYPTO-ASSETS

Digital Currency (DC):

A DC is an asset with monetary characteristics which is only available in digital, rather than physical form. DCs are considered to be both assets and value exchange mechanisms.

There are various types of DC:

- A DC is classified as e-money when it:
  - is denominated in a sovereign currency,
  - has monetary value represented by a claim on the issuer,
  - is stored electronically,
  - is issued on receipt of funds and
  - is used and accepted as payment.
- A DC is classified as a virtual currency when it:
  - Is denominated in units that are not used by legal tender backed by a central government, which is referred to as a ”fiat” currency”

Crypto-assets:

Crypto-assets is a broad term covering all assets stored on distributed ledgers. This includes all cryptocurrencies as well as non-currency assets such as security tokens and utility tokens.

Cryptocurrencies:

Cryptocurrencies are a class of digital currency that do not possess a legal status of currency or money, but can be accepted by natural and legal persons as a means of exchange and can be transferred, stored and traded electronically. A cryptocurrency is a digital representation of value, ordinarily issued and guaranteed directly by its developers or by algorithmic rules defined by its protocols (i.e. proof-of-work mining). In some circumstances, cryptocurrencies can be used to pay for goods and services and can, therefore, be seen as an alternative to money. Cryptocurrencies are typically decentralised, meaning they are not issued or guaranteed by central banks, public authorities, credit institutions, or e-money institutions; consequently, the issuance of many cryptocurrencies is not currently regulated.

Blockchain/Distributed Ledger Technology (DLT):

Crypto-assets are underpinned by blockchain technology, which is a type of DLT. A DLT functions as a database (a ledger) and/or an accounting system implemented across a network to allow participants to track the ownership and transfer of crypto-assets and tokens from one party to another in the absence of traditional financial intermediaries. The digital ledgers are maintained by participants in a decentralised network of computers.

Blockchain uses cryptography to process and verify transactions on the ledger, to make it difficult to compromise the ledger’s data and to provide independently verifiable proof of payment and ownership.

Token:

Tokens are digital representations of crypto-assets, sometimes conferred during the process of a sale with the aim of raising capital for a business or organisation. This is ordinarily achieved through an initial coin offering or security token offering (see below). Tokens are often bought in exchange for existing crypto-assets, such as bitcoin or ether. Where there is sufficient demand, some tokens are traded on a secondary market (cryptocurrency exchange platforms) and,

consequently start to carry characteristics of a payment token or cryptocurrency such as bitcoin, rather than to a utility or security token (see below).

There are two main sub-categories of token:

- Security token: Tokens designed as investment opportunities, with characteristics associated with traditional financial instruments. Examples include where the token owner anticipates future profits from the token, whether through price appreciation, interest payments or some other form(s) of profit. Security tokens are most commonly either equity or debt tokens.
- Utility/access token: these tend to be tokens which entitle the contributor to use a function, product or service provided by a particular organisation or business, for example loyalty points.

You may hear of a third category of token, known as a payment or exchange token. An example of a payment token is bitcoin; in this guidance payment tokens will be referred to as cryptocurrencies.

Mixers:

Crypto-assets are built upon different types of DLT, such as blockchain. All crypto-asset transactions are contained within the digital ledger underpinning the crypto-asset. Typically, every person with access to the digital ledger can view the transactions recorded on it. Bitcoin's ledger, for instance, can be accessed through the protocol or a website which is open to the general public.

Mixers (also known as 'tumblers') are applications which:

- aggregate crypto-asset transactions involving numerous transacting parties,
- mix the crypto-assets involved in the transactions together, and
- process the transactions.

This is done to obscure the trail of value by breaking the link between the source and destination parties of each transaction. When crypto-assets have been processed through a mixer, the digital ledger shows that a transaction was sent by one of many possible payers to one of many possible payees. Some crypto-assets achieve greater anonymity through more complicated methods of mixing.

Mixers make it possible for entities with 'tainted' crypto-assets (for instance, the crypto-asset proceeds of the sale of illegal goods online) to launder proceeds of crime by obscuring the original source of funds.

Initial Coin Offering (ICO):

An ICO (or token sale) is a fundraising tool used by businesses, where firms create a new future digital token and offer it to contributors in exchange for fiat or crypto-assets of immediate and liquid value (for example Bitcoin or Ether). Generally, tokens are created and sold in order to raise money for the business to cover its operating costs and technology development. ICOs tend to occur prior to the business platform/service being officially launched. ICOs can be public (i.e. open to any potential investor) or private (i.e. offered only to select investors). The nomenclature is deliberately close to the well-known 'IPO' in public equity markets.

In recent years, nearly 80% of ICOs have however been found to be fraudulent, where the purpose of the ICO is to defraud investors and where there is no intention to create the token, the advertised product, service or enterprise.

Tokens offered through ICOs may be subject to regulation in much the same way that securities are subject to regulation in many jurisdictions.

Security Token Offering (STO):

STOs are a category of ICOs, where the token meets the definition of security, as per the law of the particular jurisdiction. In England & Wales, for instance, the token would fall within the definition of 'specified investment', found in Part III of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).

Custodian Wallet Provider:

A digital or custodian wallet provider is an entity that provides online crypto-asset account services similar to debit card services offered by traditional financial institutions. Customers are able to use their digital wallets to hold and store crypto-assets and to transfer crypto-assets from one digital wallet to another.

In some cases, custodian wallet providers have access to mainstream payment infrastructures through partnerships with card-issuers who are licensed by companies such as VISA and MasterCard.

Cryptocurrency Exchange Platform:

These are entities engaged in exchange services between crypto-assets, tokens and fiat currencies.

Miner:

A person (an individual or entity) that runs cryptographic computations that allow new crypto-assets to be posted on the DLT. With Bitcoin, miners are rewarded for their work with a transaction fee and with newly-minted bitcoins.

TAX AND ACCOUNTING SERVICES

You may encounter customers in the crypto-asset market looking for advice in a variety of circumstances, including but not limited to:

- Calculation of taxes for crypto-assets 'earned' through mining crypto-assets such as Bitcoin.
- Calculation of taxes, including capital gains tax, for profits or gains from:
    - Sale of items in returns for cryptocurrencies or tokens;
    - Sale or exchange of cryptocurrencies or tokens;
    - Speculatively trading cryptocurrencies or tokens;
    - Holding cryptocurrencies or tokens. There are a number of reasons why an entity may hold crypto-assets. For example, individuals may have been gifted crypto-assets, which subsequently increased substantially in value over time. In terms of corporates, often hackers demand ransom payments in crypto-assets. After various high-profile attacks took place in the past five years, many companies stockpiled crypto-assets such as bitcoin in order to ensure they could pay hackers without delay should an attack occur.
- Determining the value of cryptocurrencies and tokens.
- Accounting treatment of cryptocurrencies and tokens.
- Accounting advice for typical crypto-asset businesses, such as cryptocurrency exchange platforms, custodian wallet providers and Bitcoin ATMs.
- Tax and accounting treatment for companies paying employees in crypto-assets.
- Consideration of tax implications when the entity issuing the cryptocurrencies or token in relation to the above circumstances is based in a different jurisdiction.

When you encounter customers in situations like these an analysis of the potential money-laundering risks should be performed, and if necessary, enhanced due-diligence and AML checks should be conducted.

You should bear in mind that, despite allegations of criminality concerning participants in crypto-asset markets, there are many participants in such markets that are legitimate. These legitimate participants are entitled to accounting, auditing, insolvency and tax services. The need for advisory services may be exacerbated for various reasons, including: the legal and regulatory landscape is difficult to navigate: AML/CTF laws may not yet exist in many locations; and law enforcement authorities and regulators may be reluctant to engage with market participants looking for advice on how to conduct best practices.

MONEY LAUNDERING RISKS

Before on-boarding a client associated with crypto-assets, it is necessary to understand how actors may utilise crypto-assets and tokens to commit acts of crime.

Examples of criminal actors include:

- Individual actors: for instance, an individual who buys or sells illegal goods on the dark web in return for crypto-assets;
- Small groups: for instance, individuals who are part of a small hacking group, or individuals who buy and/or sell illegal goods on the dark web with links to a larger criminal network;
- Large and/or sophisticated organisations: for instance, a group who launder crypto-asset proceeds of crime in exchange for fiat on behalf of smaller criminal organisations.

As mentioned above, there have been many ICOs which have been Ponzi schemes or were otherwise outright fraudulent. Many ICOs appear to be legitimate, with the boards of directors comprising of personnel with impressive backgrounds. Such ICOs may be organised by individual actors, small groups or much larger sophisticated groups.

Crypto-assets may be involved in any of the stages of money laundering:

- Predicate crime: for example, raising funds through illegal activity by selling illegal goods or services in return for crypto-assets.

  Placement: converting crypto-assets into fiat currencies within a traditional financial system.

  Layering: Converting fiat assets into crypto-assets, exchanging crypto-assets (including through mixers), conversion between crypto-assets and converting crypto-assets into fiat currencies. Large amounts of crypto-assets may be split into less conspicuous, smaller sums stored in many custodian wallets. These sums are then converted into fiat through cryptocurrency exchange platforms, or alternatively through 'clean' wallets in return for commission.
- Moving, converting or placing illegal funds.
- Layering fiat funds through a series of conversions or movements to distance them from their source.
- Integrating funds into the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

The following provides a worked example a case of money laundering through the use of crypto-assets:

- Traffickers sell illegal goods through the dark web in exchange for payment in bitcoin.
- Launderers advertise money laundering services for crypto-assets on a peer-to-peer forum, offering to pay cash for bitcoin from sellers looking to keep their identities secret.
- The launderers and traffickers make contact on an encrypted messaging service to discuss fees and logistics. The launderers charge crypto-asset commission in return for cashing out or exchanging the funds.
- The launderers take ownership of the traffickers' wallets, and place the crypto-assets through mixers to disguise ownership.
- The launderers pay ostensibly-innocent individuals (i.e. with no prior convictions) to open accounts with reputable banks, in addition to opening accounts using shell firms set up by corporate services providers in overseas jurisdictions.
- The launderers use local crypto-assets ATMs, which require no due-diligence, in order to exchange crypto-assets for fiat, withdraw the cash and provide it to the traffickers.
- The launderers may also use cryptocurrency exchange platforms, which require no due-diligence, to convert the crypto-assets to e-money for transfer to a custodian wallet. The e-money is then transferred into reputable bank accounts, possibly with multiple movements between bank accounts before arriving at its final destination.

Although crypto-assets are viewed as high risk, not all those associated with them are involved in criminality. Each potential client must be evaluated on its own merits, considering the AML risks associated with it and the proportionate procedures that can be put in place to mitigate those risks. In light of the example above, if faced with an enquiry from a corporate services provider with links to crypto-asset companies, it may be necessary to ascertain the type of client the provider services and assess whether it conducts adequate due-diligence on its clients (see next section).

In rapidly developing sectors such as crypto-assets, you should remember that law and regulation will be playing 'catch-up'. While a lack of a legislative framework may present an opportunity for legitimate clients to save administrative costs, it is no excuse for a failure to understand the risks of engaging with clients in a high-risk sector and failing to implement appropriate procedures to mitigate those risks.

ANTI-MONEY LAUNDERING CONSIDERATIONS

Despite crypto-assets often being described as highly disruptive and risky, when considering the AML risks associated with them it is important to remember that there are many similarities with traditional assets, e.g. cash. Whilst crypto-assets may allow greater anonymity than traditional payment methods they are, because of DLT, often inherently more transparent than cash.

Basic risk assessment questions remain the same regardless of the presence or otherwise of crypto-assets in a transaction or business relationship.

- Client risk: "Does the client or its beneficial owners have attributes known to be frequently used by money launderers or terrorist financiers?"
- Service risk: Do any of our products or services have attributes known to be used by money launderers or terrorist financiers?"
- Geographic risk: "Is the client established in countries that are known to be used by money launderers or terrorist financiers?"
- Sector risk: "Does the client have substantial operations in sectors that are favoured by money launderers or terrorist financiers?"
- Channel risk: "Does the fact that I am not dealing with the client face to face pose a greater MLTF risk?"

It may be helpful to consider the capacity in which the potential client is approaching you, and the relevance of crypto-assets to the work.

FATF regard decentralised systems as presenting a higher AML/CTF risk, being particularly vulnerable to anonymity risks, for example the bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body. It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.[1]

When dealing with persons who hold crypto-assets the primary questions will be around source of wealth and funds. Given the widespread popularity of crypto-assets, the mere presence of it in a client's portfolio does not necessarily make it a high AML risk.

Issues to consider in a risk assessment include:

- Whether the crypto-asset is known to be used by money launderers or terrorist financiers.
- Why the client has selected to be associated with the currency.
- Whether the association raises client risk.
- Whether the association raises channel risk.

[1] See page 9, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Questions include:

- Are there trading or investment records detailing the origin of the funds?
- Can the blockchain be interrogated? This may be necessary when advising companies who are considering issuing tokens through an ICO or STO.
- Have anonymising services such as mixers been used?
- Has the potential client undertaken fund transfers without the use of a third party wallet provider?
- Can a read only node be used to access the blockchain?
- Is the currency convertible or non-convertible?

FATF regard convertible virtual currencies as higher risk than non-convertible currencies. Convertible currencies can be exchanged for real money or other virtual currencies and are potentially vulnerable to money laundering and terrorist financing abuse for many reasons. First, they may allow greater anonymity than traditional noncash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.[2]

When the client (or potential client) is part of the crypto-asset system

Such clients will include those:

- issuing tokens or coins,
- fundraising via an ICO, or
- operating a crypto-asset exchange,

You should consider multiple categories of risk including:

- the reputation of the crypto-asset, its issuer(s) and exchange(s),
- the perceived level of corruption associated with the crypto-asset, its issuer(s) and exchange(s),
- the perception of criminal activity associated with crypto-asset, its issuer(s) and exchange(s), and
- the existence and effectiveness of AML/CTF controls put in place by issuers and exchange(s).

Online open source research may address some of these questions, such as:

- Who can create a wallet?
- Who can create new tokens?
- Who can see transactional details for transactions they are involved in?
- Who can see transactional details for transactions they are not involved in?
- Who can conduct/authorise new transactions?
- Are parties identified, anonymous or pseudonymous?
- Is membership open or closed?
- Does the blockchain provider have an ISAE 3402 type 2 report equivalent providing a description of its system, and assurance that controls are suitably designed and operated effectively?
- Is the currency centralised or decentralised?
- How does the token confer value; for example is it a security token, a utility token or a payment token?

[2] See page 4, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

REGULATORY ENVIRONMENT

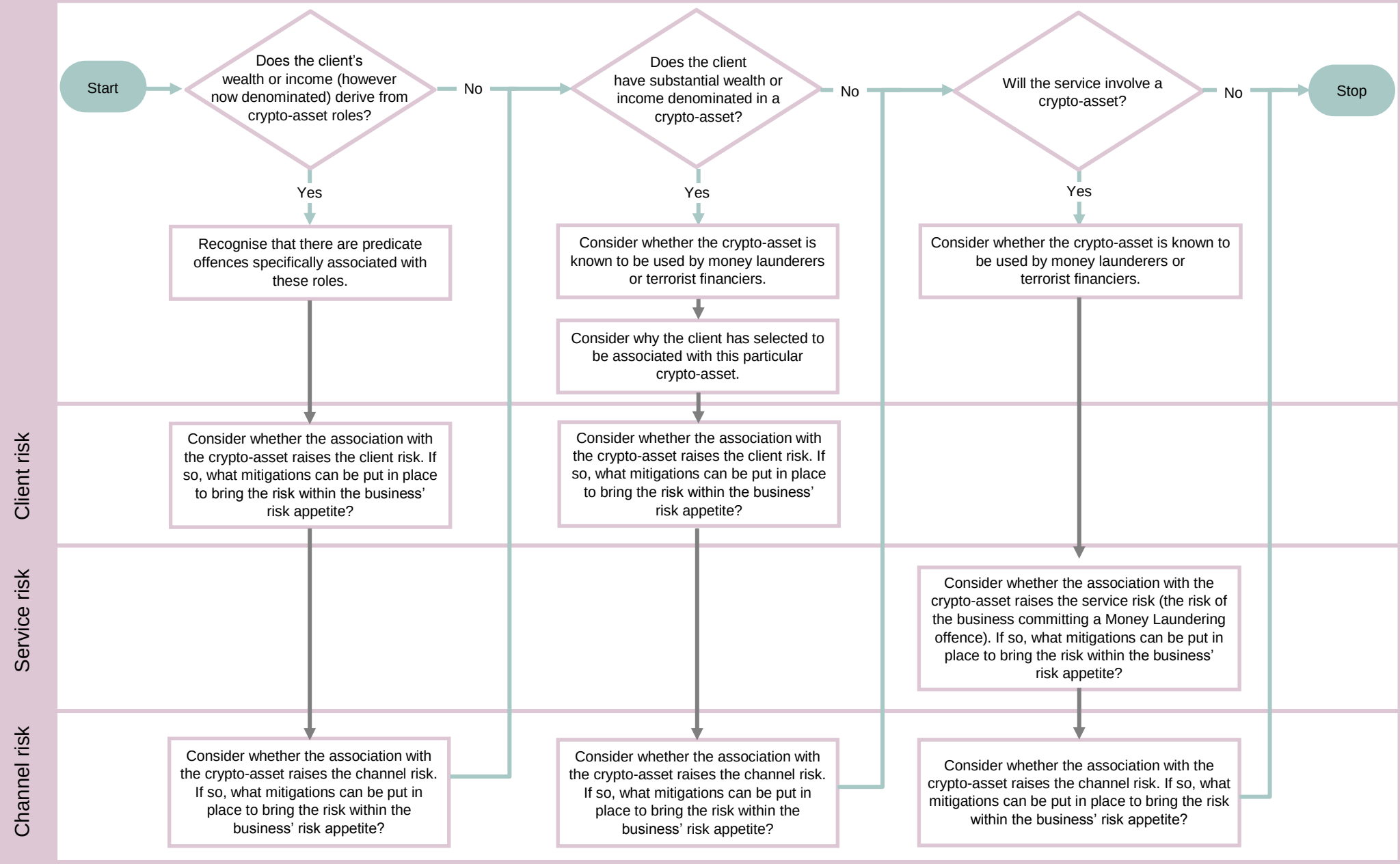
The EU has not yet implemented legislation on DLT but has adopted a directive which will see to the regulation of entities which act as gatekeepers between the fiat and crypto-asset worlds, namely cryptocurrency exchange platforms and custodian wallet providers. In July 2016, the European Commission published the directive, now known as the Fifth Money Laundering Directive (5 AMLD), which amended the Fourth Money Laundering Directive.

5AMLD introduces a definition of 'virtual currency' and requires cryptocurrency exchange platforms and custodian wallet providers to implement financial crime preventive measures, including customer due diligence, and report suspicious transactions. The European Commission takes the view that the proposed measures will address the money laundering and terrorist financing risks and will have no negative effects on the benefits and technological advances presented by blockchain technology underlying virtual currencies. The directive therefore recognises the increased popularity of virtual currencies and their potential for exploitation by criminals.

5AMLD entered into force on 9 July 2018 (the twentieth day following its publication in the Official Journal of the EU) (Article 5, MLD5). Member States must transpose the directive into national legislation by 10 January 2020 (Articles 1(42) and 4 MLD5).

Once transposed into domestic legislation this is likely to be a mitigating factor in AML risk assessment.

Assessing the Money Laundering risks associated with crypto-assets



ICAEW is a world leading professional membership organisation that promotes, develops and supports over 150,000 chartered accountants worldwide. We provide qualifications and professional development, share our knowledge, insight and technical expertise, and protect the quality and integrity of the accountancy and finance profession.

As leaders in accountancy, finance and business our members have the knowledge, skills and commitment to maintain the highest professional standards and integrity. Together we contribute to the success of individuals, organisations, communities and economies around the world.

Because of us, people can do business with confidence.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E generalenquiries@icaew.com