22: Cryptoasset exchange providers and custodian wallet providers

Note: ***This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance. This is because the sectoral guidance deals with the specific aspects of the law as it relates to cryptoasset exchange providers and custodian wallet providers; aspects of the law that relate to all obligated entities are addressed in Part I of the Guidance and are not reproduced below.***

Definitions

Cryptoasset

22.1 A cryptoasset is *a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically*, and for the purposes of the definition of a cryptoasset exchange provider *includes a right to, or interest in, the cryptoasset* (Regulation 14A(3)(a) and (c) ML Regulations).

22.2 The reference to 'a right to, or interest in, the cryptoasset' includes beneficial and security interests in cryptoassets.

22.3 Some cryptoassets may be specified investments for the purposes of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001.

22.4 Some cryptoassets may be electronic money for the purposes of the Electronic Money Regulations 2011. Firms should consider the attributes of the asset in question in order to decide whether it is electronic money. Such attributes include whether the asset constitutes monetary value, whether it is redeemable and whether it is issued on receipt of funds.

22.5 Where a cryptoasset is a specified investment or electronic money, the firm must consider whether it has the appropriate permissions under each regime and comply with relevant regulatory requirements, including those on AML/CTF. Where a cryptoasset possesses attributes associated with more than one financial instrument, firms should consider any potential overlapping obligation on a risk-based approach, taking into account the higher or more stringent obligation.

22.6 Cryptoassets include both those that are centralised, i.e., issued by an administrator, and those that are decentralised.

22.7 The definition is intended to be neutral as to the use of cryptoassets. It thus includes, amongst other types of tokens, payment, asset and utility tokens.

22.8 The definition is broad enough to include in-game currencies. A firm will need to consider whether activities related to the cryptoasset fall within the activities listed in para. 22.1 above. When doing so, the firm should take account of whether the cryptoasset can only be used within a specific game environment or whether it can also be exchanged for value that may then be used outside that environment (an exchange could take place either within the game and be followed by a withdrawal or on an exchange forum outside the game). A similar approach should be taken to closed-loop tokens such as loyalty reward points that may meet the definition of a cryptoasset.

Cryptoasset exchange provider

22.9 A cryptoasset exchange provider is *a firm or sole practitioner who by way of business provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved, when providing such services—*

(a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,

(b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or

(c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets (Regulation 14A(1) ML Regulations).

22.10 The definition of a cryptoasset exchange provider is technologically neutral.

22.11 The definition is broad, providing for exchanging as well as "*arranging or making arrangements with a view to the exchange*." This may include activities relating to a dedicated peer-to-peer platform. However, it is not intended to capture a firm that only provides a forum where buyers and sellers can post their bids and offers, such as a bulletin board where the availability of the assets are merely made known and the parties trade at an outside venue either through individual wallets or other wallets not hosted by the forum or a connected firm. Such business models will, however, be considered on a case-by-case basis.

22.12 Software developers and other providers connected to a decentralized cryptoasset exchange and payment system may fall outside of the scope of the definition, and are more likely to do so if they derive no income or benefit from consequent transactions (also see paras 22.25 and 22.26 below).

22.13 In determining the supervisory perimeter of the ML Regulations, the FCA will have regard to the policy objectives of the legislation as well as the definition itself. The following activities may, for example require assessment on a case-by-case basis:

- While mining as an activity does not as such fall within the definition of a cryptoasset exchange provider, some mining operations that carry a money laundering or terrorist financing risk may be deemed to constitute exchanges, such as when they are conducted through cloud mining or initial coin offerings;
- Services that facilitate the issuance and trading of cryptoassets on behalf of a natural or legal person's customers are intended to be captured, although this excludes the mere provision of advice or technology services;
- Escrow services in relation to cryptoasset activity, including services involving smart contract technology that buyers use to send or transfer money in exchange for cryptoassets when the firm providing the service has custody over the cryptoassets are likely to be in scope;
- The issuance of cryptoassets or their acceptance in return for goods, services, rights or actions is likely to fall outside the scope of regulation. This may, for example, be the case where cryptoassets are issued in return for click-throughs or product reviews or where they are accepted in payment for goods or services;
- Where a good or service that has been purchased with money or cryptoassets is later transformed into a cryptoasset, whether automatically or by the provider, this may be regarded as an exchange;
- The refunding of a payment made using a cryptoasset in money or a cryptoasset by a merchant that is refunded to the same payment instrument and same payment type is likely to fall outside the scope of regulation, but must again be considered in the context of the specific business.

Custodian wallet provider

22.14 A custodian wallet provider is *a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer—*

(a) cryptoassets on behalf of its customers, or

(b) private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets,

when providing such services (Regulation 14A(2) ML Regulations).

22.15 Custodian wallet providers may also offer other, related, services, such as balance checks and fee and transaction confirmation time estimates.

22.16 'To hold, store and transfer' in Regulation 14A(2)(b) is to be read cumulatively. This is meant to exclude non-custodial wallets. Therefore, firms who merely hold and store cryptographic keys, but are not involved in their transfer (the owner of the cryptoassets interacting with the payment system directly), are not likely to be in scope of the definition. This includes hardware wallet manufacturers and cloud storing service providers (together, these are 'non-custodian wallet providers') (also see paras 22.25 and 22.26 below).

Money

22.17 The ML Regulations state that *money* (for the purposes of Regulation 14A) *means—*

(i) money in sterling,

(ii) money in any other currency, or

(iii) money in any other medium of exchange,

but does not include a cryptoasset.

22.18 The third element of the definition includes electronic money. This is because electronic money constitutes monetary value, its value corresponding 1:1 to the value of the fiat currency with which it is purchased. Gift cards are also likely to be considered as money for the purposes of Regulation 14A, irrespective of whether or not they fall under the definition of electronic money.

22.19 Because cryptoassets are not currently regarded as units of account in their own right, their value is usually denominated in fiat currency. Any relevant legislative thresholds should be applied accordingly. In practical terms, firms may work out the equivalent fiat currency value of cryptoassets once a day and adjust their transaction limits accordingly.

The scope of regulation

22.20 Cryptoasset exchange providers and custodian wallet providers based in the UK are relevant persons for the purposes of the ML Regulations. They are required to register with the FCA as the relevant competent authority.

22.21 The jurisdictional scope of the ML Regulations in respect of cryptoasset providers is the same as that in respect of other relevant persons subject to the ML Regulations (see Regulations 8 and 9). In practice, application of the ML Regulations will be considered by the FCA on a case-by-case basis and is likely to differ for different business models. In most cases, application is triggered by the firm having a physical presence in the UK through which business is conducted, although other factors may also be considered. The mere fact that a firm has UK customers does not in itself mean that it would fall within the jurisdictional scope of the ML Regulations. However, a cryptoasset exchange provider that has an ATM located in the UK will be within

the scope of the ML Regulations irrespective of which jurisdiction the operator is established in or where its offices are based.

22.22 For cryptoasset exchange providers, the relevant business for the purposes of the ML Regulations is the exchange of cryptoassets and money or of cryptoassets amongst one-another. Customer-related AML/CTF obligations thus only apply to the regulated part of their business. Other business is not subject to the obligations of the ML Regulations. However, reporting obligations under the Proceeds of Crime Act 2002 (POCA) apply where the information on which a suspicion is based has been obtained *in the course of a business in the regulated sector*, and may therefore apply to all parts of the business. Cryptoassets are property under English law, bringing them within the scope of Part 7 of POCA and Part 3 of the Terrorism Act 2000.

22.23 For custodian wallet providers, the holding of money on behalf of their customers does not constitute relevant business, but may bring them within the scope of financial services regulatory regimes.

22.24 Where firms also conduct regulated activities under financial services regulatory regimes, this guidance and the relevant provisions from the ML Regulations apply in addition to their existing obligations. This may entail having to seek multiple permissions.

22.25 Software developers who merely sell an application or platform without engaging as a business in relevant activities are not included in scope.

22.26 Providers of ancillary products or services to cryptoasset networks who do not engage as a business in relevant activities are not included in scope.

22.27 The Wire Transfer Regulation does not currently apply to transfers in cryptoassets. However, firms should be aware of the FATF recommendations in this respect, and consider any relevant regulatory developments to ensure their products are compliant.

22.28 Firms whose cryptoasset activities fall outside the scope of the jurisdiction of the Financial Ombudsman Service and are not subject to protection under the Financial Services Compensation Scheme must inform their customers of this before they enter into a business relationship or carry out an occasional transaction.

What are the money laundering and terrorist financing risks in this sector?

22.29 The 2017 national risk assessment regarded the money laundering risk associated with cryptoassets as low but likely to increase and the terrorist financing risk as low and unlikely to increase. In its 2018 'National Strategic Assessment of Serious and Organised Crime,' the National Crime Agency ('NCA') found that *a small but growing number of criminals are laundering money using cryptocurrencies and anticipated that criminals will increasingly use cryptocurrencies to move illicit funds across borders*. In its 2020 assessment, the NCA found that these previously identified trends had become more prevalent in 2019 and stated that *UK-based criminals continue to identify new ways of using virtual assets, such as cryptocurrencies, to launder their profits, although more traditional methods are still favoured.*

22.30 The 2019 FATF guidance for 'Virtual Assets and Virtual Asset Service Providers' states that *while VAs may provide another form of value for conducting ML and TF, and VA activities may serve as another mechanism for the illegal transfer of value or funds, countries should not necessarily categorize VASPs or VA activities as inherently high ML/TF risks*. Instead, specific risk factors associated with the relevant products, the extent and quality of a country's regulatory framework and the implementation of risk-based controls and mitigating measures should inform the overall risk assessment.

22.31 The risk-based approach applies to the sector, which means firms should proactively assess the current and emerging risks they face and deploy their resources accordingly. Higher and lower risk factors may be set off against each other, leading to a holistic view of money laundering/terrorist financing risk.

22.32 In its 2019 guidance for 'Virtual Assets and Virtual Asset Service Providers' the FATF recognises that *in a risk-based regime, not all VASPs will adopt identical AML/CFT controls and that single, unwitting and isolated incidents involving the transfer or exchange of illicit proceeds do not necessarily invalidate the integrity of a VASP's AML/CFT controls*.

22.33 The following are factors that give rise to money laundering and terrorist financing risks (some specific to cryptoassets, others common to a number of assets) together with indicative mitigation strategies:

- **Privacy or anonymity:** The ability offered by some, unregulated, cryptoasset systems and providers to transact without being fully identified gives rise to a money laundering and terrorist financing risk.

  It should, however, be noted that the transparency and stability associated with public blockchains creates persistent, irrevocable transaction records that enable risk analysis and risk mitigation. For firms dealing with funds from anonymous or private sources, this allows for risk-based scrutiny of customers and transactions in accordance with the type of business conducted and the value and volume of transactions. Firms should consider undertaking their own analysis of the blockchain, seeking to assess any nexus to sources of risk, including the darknet and blacklisted addresses, and they should consider using the services of a specialist blockchain analysis provider, particularly where the risk is significant or the volume of transactions is substantial.

- **Cross-border nature:** the potential risks associated with a cryptoasset system's links to several jurisdictions may reduce the ability for oversight and the application of effective AML/CTF controls.

  Firms will need to ensure that they are able to effectively apply all AML/CTF processes in the jurisdictions in which they operate and compensate for any additional risk introduced by the cross-border nature of a transaction on a risk-sensitive basis.

- **Decentralised nature:** Where the cryptoasset system is decentralised, there is no central server or service provider that has overall responsibility for identifying users, monitoring transactions, reporting suspicious activity and acting as a contact point for law enforcement. This means that individuals and transactions may not be subject to risk assessment and mitigation processes equivalent to those required by AML/CTF regulation.

  Where firms deal with funds originating from decentralised systems, they should apply risk-based mitigation measures, such as blockchain analysis.

- **Segmentation:** The infrastructure used to make transfers and execute payments may be complex and may involve several entities in different jurisdictions. This increases the risk through partial oversight of cryptoasset systems and may hinder access to relevant actors by law enforcement.

  In such instances, firms should seek to work together with other parties in the value chain so as to compensate for segmentation and provide a more robust AML/CTF framework. Firms should consider whether other parties act on their behalf, as an outsourced service provider or as an agent. Firms retain responsibility for AML/CTF compliance by outsourced service providers and agents.

- **Digital nature:** The digital nature of cryptoassets means that the risks associated with non-face-to-face business relationships as well as the fast and easy movement of funds are present and need to be mitigated. This is common to all digital financial services, and a range of monitoring and digital footprint tools can be deployed to mitigate this risk.

- **Acceptability:** Where there is a wide availability of points of acceptance of cryptoassets for payment or where a large number of people are able to transact using

cryptoassets, this facilitates the use of cryptoassets for money laundering. While there is no single mitigation control, a number of measures may be employed to mitigate the arising risk.

- **Immutability:** Once a transaction has been validated, the record cannot easily be altered. This makes it more difficult for misappropriated cryptoassets to be retrieved. Users should be made aware of such risks to minimise the likelihood of accidental loss.
- **Convertibility:** The ability to exchange cryptoassets into money or other cryptoassets makes it harder to track transactions and provides a means for proceeds of crime to enter/leave the mainstream financial system. Entities can work with other parties in the value chain to address and mitigate the arising risk.
- **Innovation:** As new payment products employing emerging financial technology, cryptoassets could give rise to new types of financial crime not known with traditional payment and financial services products. Firms should work collaboratively to document and track financial crime typologies to address this risk.

22.34 The following are specific higher-risk factors that firms should have regard to in addition to the generic higher-risk factors set out in Part I, Chapter 5.5:

- The ability of users:
  - To make or accept payments in money from/to unknown or un-associated third parties;
  - To operate more than one account with the provider;
  - To operate accounts on behalf of third parties;
- The customer:
  - Is involved in cryptoasset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk cryptoassets (such as privacy coins) or where its organisation gives rise to higher risk;
  - Is a money transmitter who is unable to produce the required KYC information and documentation;
  - Uses VPN, TOR, encrypted, anonymous or randomly generated email or a temporary email service;
  - Requests an exchange to or from cash, privacy coins or anonymous electronic money;
  - Sends cryptoassets to a newly created address;
  - Persistently avoids KYC thresholds through smaller transactions;
  - Requests an exchange to or from a state-sponsored virtual currency that may be used to avoid sanctions;
  - Sends or receives cryptoassets to/from peer-to-peer exchanges, or funds/withdraws from/to money without using the platform's other features;
  - Exploits technological glitches or failures to his advantage;
- The previous or subsequent transaction is a peer-to-peer cryptoasset transfer;
- A significant proportion of the cryptoassets held or used in a transaction is associated with privacy-enhancing features or products and services that potentially obfuscate transactions or undermine a firm's ability to know its customers and implement effective AML/CTF controls, such as:
  - Mixers or tumblers;
  - Obfuscated ledger technology;
  - Internet Protocol (IP) anonymizers;
  - Ring signatures;
  - Stealth addresses;

- Ring confidential transactions;
- Atomic swaps;
- Non-interactive zero-knowledge proofs;
- Privacy coins; and
- A significant proportion of the cryptoassets held or used in a transaction is associated with second-party escrow services;

- The cryptoasset comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransom ware, hacking, fraud, Ponzi schemes, sanctioned bitcoin addresses or gambling sites;
- The results of a blockchain analysis indicate a higher risk.

22.35 The following are specific lower-risk factors:

- A low-risk nature and scope of the account, product, or service (e.g., small value savings and storage accounts that primarily enable financially-excluded customers to store limited value);
- A low-risk nature and scope of the payment channel or system (e.g., open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person/person-to-government payments);
- Product parameters or measures that lower the provider's exposure to risk, such as limitations on transactions or account balance;
- The customer requests an exchange and either the source of or destination for the money is the customer's own account with a bank in a jurisdiction assessed by the firm as low risk;
- The customer requests an exchange and either the source of or destination for the cryptoasset is the customer's own wallet that has been whitelisted or otherwise determined as low-risk;
- The customer requests an exchange and either the source of or destination for the cryptoasset relates to low value payments for goods and services; and
- The results of a blockchain analysis indicate a lower risk.

Risk management

Risk assessment

22.36 **Customer risk:**

Based on a holistic view of the information obtained in the context of their application of CDD measures, firms should be able to prepare a customer risk profile. A customer's profile will determine the level and type of ongoing monitoring necessary and support the entity's decision whether to enter into, continue, or terminate the business relationship. Risk profiles can apply at the customer level (e.g., nature and volume of trading activity, origin of virtual funds deposited etc.) or at the cluster level, where a cluster of customers displays homogenous characteristics (e.g., customers conducting similar types of transactions or involving the same virtual assets).

Firms should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD.

All customers should be screened against appropriate industry-specific blacklists in accordance with industry practice.

Where firms deal with commercial counterparties in the same sector, they may employ a number of measures to assess the risk associated with the relationship, including the hiring of investigators to test the counterparty's AML controls, consideration of any information shared or in the public domain about the counterparty, assessment of the equivalence of local legislation and consideration of contractual arrangements between the counterparty and its customers, such as whether entities supplying cryptoassets are contractually committed to backing the assets.

22.37 **Product risk:**

The features of the service offered as well as the actual cryptoasset which customers may hold, store, transfer or exchange determine the overall risk associated with the product. Any changes to the service or cryptoassets offered should be assessed for their impact on risk prior to their introduction.

22.38 **Transaction risk:**

The risk of a transaction is established by analysing the blockchain to obtain transaction information. The transaction is scored for its risk by investigating the provenance of the relevant tokens, establishing the time that has elapsed since any higher-risk event and the proportion of higher-risk tokens within the transaction.

Blockchain analysis (also called blockchain tracing) is sometimes outsourced to an external service provider (for guidance on outsourcing, see Part I, paras 2.16ff). Outsourcing does not remove the firm's responsibility under the ML Regulations, and firms should ensure that they undertake due diligence on the outsourced service and provider when integrating that service into their business activities. Whether to employ blockchain analysis, the degree of analysis and the use of third parties should be decided using a risk-based approach.

22.39 **Geographical risk:**

Geographical risk relates both to the customer's place of establishment and the provenance of the cryptoasset. Where information about the destination of funds is collected, this will also inform the assessment of geographical risk.

Apart from the requirements relating to transactions and relationships involving high-risk third countries (see Part I, para. 5.5.11), firms should take into account publicly available information about the regulatory treatment and use of cryptoassets in particular jurisdictions to assess geographical risk.

22.40 **Delivery channel risk:**

The risks related to how customers access the firm's products or platform need to be considered. For example, whether they are only accessible online or whether ATMs or other physical infrastructures are being used. The potential risks associated with the presence of an intermediary between the cryptoasset exchange provider and the customer may also need to be considered in this context, although blockchain analysis (or similar processes) may mitigate any associated risks to a certain extent.

Risk mitigation

22.41 The following risk mitigation measures may be employed:

- Transaction limits, including limits on the total value of privacy coins that may be held, stored, transferred or exchanged;
- Time delays before certain automated and manual transactions can be carried out with a view to restrict the rapid movement of funds, where the delay implemented will depend on the product in question and associated risk typologies; and

- The prohibition of transfers of money to third parties (i.e., the name on source and destination accounts must match where money is exchanged for cryptoassets or cryptoassets for money).

Customer due diligence ('CDD')

Who is the customer?

22.42 For cryptoasset exchange providers, the customer is generally the person requesting the exchange, regardless of the means of doing so.

22.43 For custodian wallet providers, the customer is generally the person on behalf of whom they hold, store and transfer a cryptoasset.

22.44 Where a cryptoasset exchange provider or custodian wallet provider is a client of another institution that is subject to the ML Regulations, the cryptoasset firm is that institution's customer, unless there is evidence to the contrary. CDD on that cryptoasset firm should be undertaken on a risk-sensitive basis in line with the provisions for non-regulated businesses that are subject to the ML Regulations in Part I, paras 5.3.139ff. If the relationship with the cryptoasset firm has characteristics similar to a cross-border correspondent banking relationship, the institution may need to consider the risk factors and associated guidance set out in Part II, Sector 16 when applying CDD.

The application of CDD measures (see Part I, Chapter 5)

22.45 CDD measures must be applied to all business relationships. It is likely that most cryptoasset transactions will be undertaken as part of a business relationship.

22.46 CDD measures must also be applied to occasional transactions (single or linked) of EUR 15,000 or more. However, this threshold does not apply to cryptoasset exchange providers in as far as they are operating an ATM, in which case CDD measures must be applied to all transactions.

22.47 Occasional transactions are transactions not carried out as part of a business relationship, (i.e., where there is no expectation that the firm will establish an ongoing relationship with the customer). For the distinction between occasional transactions and a business relationship, also see Part I, para. 5.3.7.

22.48 In addition, CDD measures are required where the firm suspects money laundering or terrorist financing, or where it doubts the veracity or adequacy of documents or information previously submitted for CDD.

22.49 Firms must also apply CDD measures:

- At other appropriate times to existing customers on a risk-based approach; and
- When they become aware that the circumstances of an existing customer relevant to their risk assessment for that customer has changed.

CDD and related measures

22.50 CDD and other measures employed by cryptoasset exchange providers and custodian wallet providers can typically include the following:

- Know your customer ('KYC');
- Blockchain analysis;
- Source and destination of funds: and
- Ongoing monitoring.

KYC

22.51 KYC includes identifying and verifying the customer's identity, assessing the purpose and intended nature of the business relationship or occasional transaction and identifying and taking reasonable measures to verify the identity of beneficial owners (see Part I, Chapter 5).

22.52 The information collected as part of the KYC processes may include wallet addresses and transaction hashes.

22.53 For measures to mitigate the risk of impersonation fraud for non-face-to-face transactions and relationships, see Part I, paras 5.3.85ff.

22.54 Given the potential involvement of multiple regulated firms in cryptoasset transactions, it may be helpful for firms to develop reliance or outsourcing agreements on a bilateral basis in order to minimise duplication of KYC processes and improve the customer experience.

Blockchain Analysis

22.55 Blockchain analysis processes are additional to the KYC processes required by the ML Regulations and take account of the unique opportunities afforded to cryptoasset exchange providers and custodian wallet providers by the blockchain. Blockchain analysis helps these providers assess the risk of transactions. Firms should consider how blockchain analysis may be appropriate to apply in line with a risk-based approach, including taking into account the nature of the business of the exchange provider and whether it would be appropriate to use it for all transactions.

Source and destination of funds

22.56 Evidence of the source of funds and wealth must be collected with respect to all transactions that present a higher risk, including those that involve:

- An exchange of cryptoassets for money or vice versa;
- An exchange of one cryptoasset for another if the customer claims the cryptoasset has been obtained through mining; and
- The transfer of a customer's cryptoassets from one exchange to another.

For transactions carried out under a business relationship, this evidence may only need to be collected once.

22.57 Evidence of the source of funds/wealth is also part of EDD processes (see Part I, paras 5.5.1ff).

22.58 Information about the destination of funds is not currently required by law, but it is good practice to collect this in order to inform the assessment of risk (e.g., geographical risk) and aid transaction monitoring processes. Where a recipient's name has been collected, sanctions obligations apply in the usual way (see paras 22.71-22.72 below).

Ongoing monitoring

22.59 In addition to the usual ongoing monitoring requirements that apply to business relationships (see Part I, paras 5.7.1ff), all transactions must be monitored for unexpected behaviours and indicators of suspicious activity, particularly where the interface between cryptoassets and money is concerned.

22.60 Ongoing monitoring systems should include consideration of the parties the customer is transacting with.

Simplified due diligence ('SDD')

22.61 If cryptoasset exchange providers and custodian wallet providers determine that the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing, the firm may apply SDD measures (see Part I, paras 5.4.1ff). It is, however, anticipated that SDD will apply only in limited circumstances. Where SDD measures are applied, the firm should clearly document the risk assessment undertaken in order to make this determination.

Enhanced due diligence ('EDD')

22.62 In addition to the EDD measures detailed in Part I, para. 5.5, EDD measures specific to this sector include:

- Corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;
- Searching the Internet for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with UK privacy legislation;
- Tracing the customer's IP address; and
- Requesting data relating to transaction and trading history.

Record keeping

22.63 Record keeping requirements apply to cryptoasset exchange providers and custodian wallet providers (see Part I, Chapter 8).

22.64 Records should include:

- The information relating to the identification and verification of relevant parties;
- The public keys (or equivalent identifiers) of relevant parties;
- The addresses or accounts involved (or equivalent identifiers);
- The nature (e.g., deposit, transfer, exchange) and date of transactions; and
- The amounts transferred.

22.65 While the public information on the blockchain or other relevant distributed ledger of a particular cryptoasset may provide a basis for recordkeeping, reliance solely on the blockchain or other type of distributed ledger underlying the cryptoasset for record keeping purposes is not sufficient.

Dealing with suspicious transactions

22.66 Suspicious activity reporting requirements apply to cryptoasset exchange providers and custodian wallet providers (see Part I, Chapter 6 and para. 22.22 above).

22.67 Where a firm detects suspicious activity under POCA, in relation to an incoming transfer of cryptoassets from an external party that cannot be stopped due to processes associated with the blockchain, the firm should restrict the actions that can be performed by its customer in relation to the suspicious funds, freeze the assets/funds (where possible) and report the suspicious activity.

22.68 For the sake of a holistic approach, it is noted that where the firm's services facilitate the trading of cryptoassets on behalf of a natural or legal person's customers, and suspicious activity related

to market abuse is identified, the firm should file a suspicious transaction and order report (STOR) (refer to Sector 18).

22.69 Firms should implement the necessary controls to hold incoming cryptoassets deemed suspicious and ensure that they are not released to their customers until necessary clearance has been granted by the NCA. Such controls may involve a pooled account where all uncleared cryptoassets are kept or a hold/ledger balance similar to that of bank accounts.

22.70 If a firm needs to reject or refund a transaction, it should initiate a new transaction to return the cryptoassets to its sender or legitimate owner.

Sanctions screening

22.71 Sanctions obligations apply to cryptoasset exchange providers and custodian wallet providers as they do to other firms (see Part III for details).

22.72 Firms should be aware that some sanction lists may now include information on wallet numbers in addition to/instead of names.