ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Virtual Asset Service Provider Activity

Sector Specific AML/CFT Guidance Notes

December 2024

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

Version history

Version 2 (April 2020)	Updates made to links in relation to the updated NRA
Version 3 (August 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes. 2 - Addition of further FATF reference papers 3 – Addition of further red flags following the publication of additional FATF reference papers 5 – removal of references to simplified customer risk assessment
Version 4 (December 2024)	Updates to reflect the change in terminology and definitions. Wording added around the provision of 'Financial Services' in relation to the VASP sector. Links have been updated to reflect the most up to date FATF guidance and documentation. Refreshed to better align with evolving international standards.

1. Foreword

This guidance is applicable to businesses conducting Virtual Asset Service Provider ("VASP") activity, which includes the activity of an Intermediary Virtual Asset Service Provider ("IVASP").

The activity of a VASP is included in paragraph 2(6)(r) of Schedule 4 to the Proceeds of Crime Act 2008 ("POCA") and is defined as follows:

> **"virtual asset service provider"** or **"VASP"** means any natural or legal person who by way of business conducts one or more of the following activities or operations for or on behalf of another natural or legal person **–**
>
> a. Exchange between virtual assets and fiat currencies;
> b. Exchange between one or more forms of virtual assets;
> c. Transfer of virtual assets;
> d. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
> e. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

The activity of an IVASP is included in paragraph 4 of the Travel Rule (Transfer of Virtual Assets) Code 2024 ("the Travel Rule Code") and is defined as follows:

> "**intermediary virtual asset service provider**" means a virtual asset service provider that provides exchange, transfer or safekeeping and/or administration services to, or for, the virtual asset service provider of the originator or beneficiary but does not have a business relationship with either the originator or the beneficiary.

By virtue of being included in Schedule 4 to POCA, a business conducting the activity of a VASP is subject to the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code"). Also, this sector is included in the Designated Businesses (Registration and Oversight) Act 2015 ("the DBROA") which came into force in October 2015. The sector's inclusion in the Designated Business regime gives the Financial Services Authority ("the Authority") the power to oversee VASPs for Anti-Money Laundering and Countering the

Financing of Terrorism ("AML/CFT") purposes. The sectors subject to the designated business regime can be found in Schedule 1 to the DBROA.

Further, the VASP sector is also now subject to the requirements of the Travel Rule Code that came into effect in October 2024 and which mandates certain originator and beneficiary information to be transmitted with a virtual asset transfer.

Any person seeking to provide VASP services, in or from the Isle of Man ("the Island"), should obtain relevant independent legal advice to ensure that the proposed activities are subject to the appropriate framework i.e. whether the activity is designated business under the DBROA, or whether the activity may be licensable under other legislation such as the Financial Services Act 2008 ("the FSA08").

2. Introduction

The purpose of this document is to provide guidance specifically for the VASP sector in relation to AML/CFT. This document should be read in conjunction with the Code, the main body of the AML/CFT Handbook ("the Handbook"), the Travel Rule Code and the separate Travel Rule Code Guidance document.

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across sectors.

"**financing of terrorism**" includes the **financing of proliferation** and is to be construed in accordance with the definitions of "**financing**", "**terrorism**" and "**proliferation**" in section 3 of the Terrorism and Other Crime (Financial Restrictions) Act 2014.

This document includes references to the following Financial Action Task Force ("FATF") documents:

FATF reports:	**Date of issue**
Guidance for a risk-based approach – Virtual Assets and Virtual Asset Service Providers	October 2021
Second 12-Month review of the revised FATF Standards on Virtual Assets and Virtual Asset Service Providers	July 2021

Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing	September 2020
12-Month review of the revised FATF Standards on Virtual Assets and Virtual Asset Services Providers	June 2020
Guidance for a risk-based approach – Virtual Currencies	June 2015
Virtual Currencies – Key definitions and potential AML/CFT Risks	June 2014

The Authority recommends that relevant persons familiarise themselves with these documents and other typology reports concerning this sector. Also, some case studies are included in this document to provide context to the risks of the sector.

2.1 National Risk Assessment

The Island's National Risk Assessment ("NRA") was first published in 2015 and was updated in 2020. VASPs must ensure their business risk assessment ("BRA") (and customer risk assessments ("CRA") where necessary) take any relevant findings of the NRA into account.

At the time of publication of this document, the NRA is currently undergoing a revision. Further to this, a standalone VASP Sector Risk Assessment will be produced, and relevant persons should ensure that this, along with any other sectoral or topical risk assessment that may be pertinent to VASPs or virtual assets, are considered when reviewing their own policies and procedures including their BRA.

The VASP sector is evolving and exhibits its own key risks and vulnerabilities. It is the responsibility of VASPs to keep up to date with developments and any relevant case studies. This sector presents challenges in relation the level of regulatory (and investigatory) expertise in the field and keeping up with how this sector evolves.

Services of this type provide a level of anonymity greater than traditional non-cash methods and can present a difficulty in linking an "account" to a real identity. VASPs should carefully consider features, products or services that potentially disguise transactions or hinder CDD and related measures and ensure business relationships are in compliance with the requirements of the Code at all times.

A number of control measures have been put in place through the Code, however there are a number of ML and FT risks within the sector (some of which are covered above) that cannot easily be mitigated. Therefore, ML risk for VASPs on the Island is assessed as medium high and the FT risk as medium (as at the 2020 NRA). This will be updated accordingly when both the VASP Sector Risk Assessment and the refresh to the NRA has been completed in 2025.

2.2 Terminology

There are a number of terms used when describing concepts within this sector. The following definitions are those used by the FATF (unless otherwise stated):

Virtual Asset Service Provider section 1 of this document provides the Island's legislative definition of this term. The decision to adopt a new sectoral definition in 2024 was taken to better align our framework with the global standards set by the FATF.

Digital currency refers to any electronic representation of a fiat currency and can include representations of virtual currency.

Fiat currency a.k.a. "real currency" or "real money" is a national currency that is not pegged to the price of a commodity such as gold or silver. Fiat currency is generally issued by a country's government or central bank and is designated as legal tender.

Non-convertible virtual currency, once purchased, cannot be transferred to another person and cannot be redeemed for fiat currency, either directly or through an exchange. (Note that the definition of VASP included in Schedule 4 to POCA does not extend to non-convertible currency businesses).

Virtual Asset refers to 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, securities, and other financial assets.

2.3 Context of the sector

By way of a breakdown of activity on the Island, registered VASPs typically undertake the following types of activity:

1. **buying, selling, exchanging or otherwise trading between virtual assets and fiat currencies** – allowing customers to exchange fiat currency for virtual assets and vice versa, as well as trading between different virtual assets.

2. **issuing, transmitting and transferring in respect of an Initial Coin Offer ("ICO") and exchange between one or more forms of virtual assets** – allowing customers to exchange between different forms of virtual assets, a token, or coin to raise funds for a particular product or software/service (typically blockchain). The token or coin purchased at the time of the ICO usually brings with it a benefit to the purchaser once the ICO is complete, for instance the token or coin is discounted at various times

throughout the ICO (bigger discounts for early take-up and for higher amounts purchased).

3. **transfer of virtual assets** - allowing customers to transfer ownership or control of virtual assets to another user, or to transfer virtual assets between virtual asset wallet addresses or accounts held by the same user.

4. **safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets** – the term "*safekeeping*" consists of the service of holding a virtual asset or the private keys to the virtual asset on behalf of another person. The term "*administration*" could also include the concept of managing virtual assets for, or on behalf of, another person. The term "*control*" should be understood as the ability to hold, trade, transfer or spend the Virtual Asset. Parties that can use a virtual asset or change its disposition have control of it.

5. **participation in and provision of financial services related to an issuer's offer and /or sale of a virtual asset** - covers persons who participate in, or provide related financial services to, issuer's offer and/or sale of virtual assets through activities such as ICOs. This could include, for example, businesses accepting purchase orders and accompanying funds, and purchasing virtual assets from an issuer to resell and distribute the funds or assets. Also, possible market making for ICOs and acting as a placement agent for ICOs.

Item 5 above refers the provision of '**financial services**' related to an issuer's offer and/or sale of a virtual asset. The term 'financial services activity' is defined in the FSA08 and refers to the activity of:

a. deposit taking
b. investment business
c. any service to a collective investment scheme
d. corporate services
e. trust services
f. crowdfunding platforms
g. any service or activity involving money transmission
h. any other financial service or financial activity of a specified kind that is carried on by a person of a specified description.

If the VASP were undertaking any of the activities defined as 'financial services activity' in the normal course of their business, then there would be a requirement for the firm to apply to be licensed under the FSA08. The VASP would then be subject to full regulatory oversight and the conditions of the financial services rule book.

If a VASP believes they may be undertaking activities that would constitute 'financial services activity' then please contact the Authority to arrange a meeting to discuss further.

2.4 Non-Fungible Tokens

Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as a non-fungible token ("NFT"). Such assets, depending on their characteristics, are generally not considered to be virtual assets under the definition.

It is, however, important to consider the nature of an NFT and its function in practice and not just the terminology or the marketing terms that are used to promote it. Some NFTs, that on the face of it, do not appear to constitute a virtual asset may fall under the virtual asset definition if they are to be used for payment or investment purposes in practice.

The characteristics and function of an NFT should be considered on a case-by-case basis when determining whether it is captured within the scope of the virtual asset definition, and therefore subject to the requirements of the legislation.

3. Risk Guidance

The Code mandates that a number of risk assessments are completed:

- a business risk assessment (paragraph 5)
- a customer risk assessment (paragraph 6)
- a technology risk assessment (paragraph 7)

As demonstrated by the descriptions in section 2.3, the VASP sector is broad and the ML/FT risks will vary for each business based on a wide range of factors such as the type of products they supply, their customers and delivery channels. One particular matter to consider is the fact that VASPs enable non-face-to-face business relationships. VASPs can also be used to quickly move funds globally and to facilitate a number of financial activities[1]. Factors such as this can indicate higher ML/FT risks, these risks are further compounded by the potential for anonymity behind the transactions. Diligence is required for any business in this sector to take

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

appropriate steps to keep knowledge up to date, given that both the sector and the risks are constantly evolving.

Vigilance should govern all aspects of the business' dealings with its customers, including: -

- compliance with the Travel Rule Code.
- on-boarding / account opening.
- virtual asset screening.
- the receipt of customer instructions.
- transactions into and out of the customer account (or wallet).
- ongoing monitoring of the business relationship.
- technology / security issues in relation to the online element to the business relationship.
- where any services are outsourced or delegated.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship high risk, the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which may cause it concern, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;
(b) conduct EDD in accordance with paragraph 15; and
(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and
(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures.

Also, please see the list of red flags included at 3.2 of this document.

High risk indicators:

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the business with complete information about the nature and purpose of the relationship including anticipated account activity.
- The customer uses anonymiser software, a mixer or similar system to obscure the true identity of the remitter.
- The customer is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc. especially if the customer is otherwise secretive or avoids direct contact.
- The customer is located in a higher risk jurisdiction.
- Transactions involving numerous jurisdictions.
- The customer is reluctant to meet personnel from the firm in person and / or uses a "front person".
- The customer has no discernible reason for using the businesses' services, or the businesses' location.
- The customer's address is associated with multiple accounts that do not appear to be related.
- The customer frequently changes their identification information, including email addresses, IP addresses, or financial information.
- Where the customer does not appear familiar with the technology utilised by the business or is significantly older than the average age of platform users and engages in large numbers of transactions.
- There is an excessively high or low price attached to the virtual asset transferred, with regard to any circumstance indicating such an excess (e.g. volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation.
- The customer is suspected to be experiencing extreme financial difficulties.
- The nature of activity does not seem in line with the customer's usual pattern of activity.
- The customer enquiries about how to close accounts without explaining their reasons fully.
- The customer opens an account / product without any regards to loss, commissions or other costs associated with that account / product.
- The customer exhibits unusual concern with the businesses' compliance with Government reporting requirements and/or AML/CFT policies and procedures.

- The customer funds deposits, withdraws or purchases financial / monetary instruments below a threshold amount to avoid certain reporting / record keeping requirements.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. If a relevant person identifies suspicious activity, as explained in section 3 of this document, and the Code, appropriate steps must be taken. The below list of potential red flags is by no means exhaustive:

- Where it is identified a customer provides false or misleading information.
- Where it is identified a customer provides suspicious identification documents.
- The customer does not provide the business with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity.
- The customer is secretive / evasive when asked to provide more information.
- When requested, the customer refuses to identify a legitimate source of funds or source of wealth.
- The customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect.
- The customer enquiries about how quickly they can end a business relationship where it is not expected.
- Where the requirements of the Travel Rule Code are routinely not being complied with.
- Where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question.
- The customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for.
- Where the customer is attempting to convert a virtual asset which has a significant proportion of dark web activity.
- The customer is known to have criminal / civil / regulatory proceedings against them or is associated with such persons.
- the customer is interested in paying higher charges to keep their identity secret.
- Cannot or will not commit to fulfilling their obligations in respect of the Travel Rule Code.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to the VASP sector. Some of these have been included from this FATF reference paper. Further guidance surrounding the risk assessments is outlined in chapter 2 of the Handbook.

This will be updated upon publication of the 2025 NRA.

3.3.1 Technology risk

Due to the nature of the rapidly evolving sector, particular focus should be given to the technology risk assessment ("TRA"). This must assess the risk of ML/FT posed by any technology utilised by the business, such as the use of online delivery channels and communication methods, to its business. A TRA should also be undertaken in respect of any third-party provider used by a VASP or relevant person to meet the requirements of the Travel Rule Code. The BRA must also take the TRA into account.

3.3.2 Anonymity

As stated in paragraph 40 of the Code:

> **40 Fictitious, anonymous and numbered accounts**
> A relevant person must not set up or maintain an account in a name that it knows, or has reasonable cause to suspect, is fictitious, an anonymous account, or a numbered account for any new or existing customer.

The following list, which is not exhaustive, includes some factors to consider in relation to anonymity when undertaking VASP and virtual asset activity:

- Virtual asset activity is associated with greater anonymity than traditional non-cash payment methods and therefore could be used to facilitate anonymous funding.
- It is traded on the internet, typically by non-face-to-face customer relationships.
- It may also result in anonymous transfers if sender and recipient are not adequately identified.
- Decentralised virtual asset payment providers are particularly vulnerable to anonymity risks. For example, wallet addresses functioning as accounts may have no names or other customer identification attached by design, and the system has no central server or service provider.
- A VASP in another jurisdiction may not require a user to provide identification and verification, and/or the historical transaction records generated on the blockchain are not associated with real world identity.

- The anonymity of many decentralised virtual asset transactions limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity and presents a significant challenge to achieving effective AML/CFT compliance.
- Decentralised VASPs have no central oversight body and while AML compliance software is being developed to monitor and identify suspicious transaction patterns, it is not yet commercially tested and available.
- Software products have been developed to enhance decentralised VASP anonymity features, including coin mixers and IP address anonymisers. Use of these tools may make application of CDD measures nearly impossible.

3.3.3 Global reach and disaggregation

The following list, which is not exhaustive, includes some factors to consider in relation to the global reach of VASP activity: -

- Services can be accessed via the internet (including via mobile phones) and can be used to make cross-border payments to anywhere in the world, including higher risk jurisdictions; these payments could potentially be in breach of sanctions.
- Some VASPs rely on complex infrastructures involving several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance, supervision and enforcement may be unclear or non-existent in some jurisdictions.
- Customer and transaction records may be held by different entities, often in different jurisdictions, therefore making it more difficult for law enforcement, regulators and supervisors to access them.
- The rapidly evolving nature of decentralised virtual asset technology and business models, including the varying numbers of providers and differing roles of participants providing VASP payment services.
- Operations of a VASP may be located in jurisdictions that do not have adequate AML/CFT controls.
- Decentralised VASPs, allowing anonymous person-to-person transactions, may seem to exist in a digital universe entirely outside the reach of any particular jurisdiction.
- Centralised VASPs may be wilfully complicit in criminal activities. See case study (Liberty Reserve) illustrated at section 8.1 of this document.

3.3.4 Other risk factors

The following list, which is not exhaustive, includes some factors to consider in relation to some other risk factors when undertaking VASP or virtual asset activity: -

- The near real-time settlement and irrevocability of transactions (no chargebacks).

- Challenges in tracing the flow of virtual assets and freezing or seizing illicit proceeds held in the form of virtual assets due to data encryption.
- Lack of mechanism to delay, freeze, return or decline transactions to or from hosted addresses in the event of suspicious activity, court orders etc.
- VASP developers and providers may come from non-financial services backgrounds, which are not as highly regulated or mature as the financial sector in terms of AML/CFT. Therefore, the businesses may be less aware of the risks posed by their products, applicable AML/CFT requirements and lack experience in complying with them. Additionally, consideration should be given to the fact that the VASP sector is constantly evolving.
- Software updates or 'forks' bringing new technical features to a blockchain, consideration should be made if any such updates present additional ML/FT risks.
- Many jurisdictions do not have an existing AML/CFT framework for VASPs and as such, Island based VASPs may be exposed to higher levels of risk by having customers, business partners or agents who are based outside of this jurisdiction.
- Generally higher risk factors as discussed in this document make VASPs vulnerable to abuse by those looking to exploit for ML/FT purposes.

4. Travel Rule

The Travel Rule Code came into operation in October 2024. This obliges VASPs operating, in or from, the Island to comply with requirements of FATF Recommendation 16 in respect of originator and beneficiary information connected to the transfer of virtual assets.

The primary purpose of the Travel Rule Code is to compel relevant persons (including VASPs) to transfer certain customer identification information when sending or receiving virtual assets.

Further information about the Travel Rule Code can be found in the separate Travel Rule Code Guidance document.

5. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships. Chapter 3 of the Handbook provides guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided. For details of particular concessions which may be applicable please see chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 8(5), 9(9), 10(5), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must provide that -

(a) the business relationship must proceed no further;
(b) the relevant person must consider terminating[2] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

5.1 Source of funds

Paragraph 8(3)(e) of the Code requires the taking of reasonable measures to establish the source of funds for all new business relationships.

8 New business relationships

(e) taking reasonable measures to establish the source of funds, including where the funds are received from an account not in the name of the customer —

(i) understanding and recording the reasons for this;

(ii) identifying the account holder and on the basis of materiality and risk of ML/FT taking reasonable measures to verify the identity of the account holder using reliable, independent source documents, data or information; and

(iii) if the account holder is assessed as posing a higher risk of ML/FT, satisfying the requirements in paragraph 15.

Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth.

The Authority considers that this includes any account number or reference (or similar), the name of the remitter (as to identify whether first- or third-party funding) and the geographical source.

The source of funds will typically be from the customer themselves or from a third party. Where funds are being paid by a third party, the relevant person must identify and take reasonable measures to verify the identity of this third party where necessary, as per paragraphs 8(3)(e) and 11(3)(e) of the Code. It should also seek to establish the relationship between the customer and the third party and must understand and consider the rationale for the payment and whether this appears reasonable.

Where the source of funds is a virtual asset address (or similar numbered remitter), reasonable steps should be taken to determine the source of the virtual asset. Determining

[2] In relation to a new business relationship (paragraph 8) the business relationship must be terminated.

the source of the funds may take the form of a disclosure from the customer explaining the source of the funds. Should this explanation appear not to make sense based on the known information about the customer, then further investigation must be undertaken to establish the source of the funds as per the requirements of the Code.

5.2 Enhanced due diligence

Paragraph 15 of the Code requires enhanced due diligence to be undertaken in certain circumstances, for example in relation to a higher risk customer and where unusual and / or suspicious activity is identified. Paragraph 15(2) states enhanced due diligence includes:

15 Enhanced due diligence

(a) considering whether additional identification information needs to be obtained and, if so, obtaining such additional information;
(b) considering whether additional aspects of the identity of the customer need to be verified by reliable independent source documents, data or information and, if so, taking reasonable measures to obtain such additional verification;
(c) taking reasonable measures to establish the source of the wealth of a customer;
(d) undertaking further research, where considered necessary, in order to understand the background of a customer and the customer's business; and
(e) considering what additional ongoing monitoring should be carried out in accordance with paragraph 13 and carrying it out.

In addition to the above steps required by the Code, enhanced due diligence measures that may mitigate the potentially higher risks associated with this particular sector could include:

- Corroborating the identity information received from the customer, such as a national identity number, and information in third-party databases or other reliable sources.
- Potentially tracing the customer's IP address.
- Searching the Internet for information to corroborate that the activity is consistent with the customer's transaction profile, provided that the data collection is in line with national Data Protection legislation.

Further guidance on enhanced due diligence is at section 3.4.7 of the Handbook.

6. Blockchain Analytics Solutions

Relevant persons should consider making use of Blockchain Analytics solutions to help inform their business and customer risk assessments. Whilst the Authority is technology neutral, it recognises the important role innovative technology can play, especially given the nature of the VASP sector.

These solutions can help provide relevant persons engaged in virtual asset transactions with a more informed and risk-based understanding of the history behind a virtual asset, and the identification of ML/FT suspicions connected with a virtual asset transfer.

Any new technology would be subject to a TRA in accordance with paragraph 7 of the Code (see section 3.3.1 of this document).

7. Simplified customer due diligence measures

The following section sets out further detail regarding concessions that may be applicable to the sector.

7.1 Exempted occasional transactions

Paragraph 11(5) of the Code provides a concession that the verification of identity is not required for customers carrying out an "exempted occasional transaction".

An exempted occasional transaction is defined in the Code as follows: -

> **3 Interpretation**
>
> (1) **In this Code -**
>
> **"exempted occasional transaction"** means an occasional transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or, the aggregate in the case of a series of linked transactions, is less in value than —
>
> a) €5,000 in relation to an activity being undertaken which is included in Class 8(1) (bureau de change) and Class 8(3) (cheque encashment) of the Regulated Activities Order;
>
> b) **€1,000** in relation to an activity being undertaken which is included in Class 8(4) (money transmission services apart from cheque encashment) of the Regulated Activities Order **and paragraph 2(6)(r) (virtual asset service provider)** of Schedule 4 to the Proceeds of Crime Act 2008; or
>
> c) €15,000 in any other case;

If the conditions are met and this concession is utilised, the verification of the customer's identity is not required. However, all other Code requirements such as paragraphs 6, 13, 14 and 15 continue to apply.

This concession is typically used by VASP entities (where the conditions are met) where a customer: -

- Participates in an ICO within the exempted occasional transaction amount.
- Participates in an exchange within the exempted occasional transaction amount.
- Purchases a utility token within the exempted occasional transaction amount.

Further information about exempted occasional transactions can be found in section 4.1 of the Handbook.

8. Case Studies

The case studies below are real life examples of risks that have crystallised causing losses and or sanctions (civil and criminal) against the sector. These examples are based on publicly available sources and FATF typology papers relating to this sector.

8.1 Liberty Reserve

In May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA Patriot Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars ("LR"), but at each end, transfers were denominated and stored in fiat currency (typically US dollars).

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers," "Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made-up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits

and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable.

After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.

8.2 Silk Road

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million Bitcoins) and approximately USD 80 million (more than 600 000 Bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were laundered from these illegal transactions (based on Bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of the total sale price.

Silk Road achieved anonymity by operating on the hidden Tor ("The onion router") network and accepting only Bitcoins for payment. Using Bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer ("P2P") Bitcoin transactions are identified only by the anonymous Bitcoin address/account. Moreover, users can obtain an unlimited number of Bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional "anonymisers," beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained Bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's Bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's Bitcoins from the escrow account to the vendor's Silk Road Bitcoin address.

As a further step, Silk Road employed a “tumbler” for every purchase, which, as the site explained, “sent all payments through a complex, semi-random series of dummy transactions, making it nearly impossible to link your payment with any [bit] coins leaving the site.” [sic]

In September 2013, the US Department of Justice shut down the website and arrested the founder. The Justice Department seized approximately 173 991 Bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware.

In November 2013 Silk Road 2.0 came online, run by former administrators of Silk Road. It was also shut down, and the alleged operator was arrested on 6 November 2014. The founder of Silk Road was convicted of seven charges related to Silk Road in the U.S. Federal Court in Manhattan and was sentenced to life in prison without possibility of parole.

8.3 Western Express International

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyber fraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet “carding” web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and Web Money. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the buyers. The money mover laundered the cybercrime group’s illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group’s proceeds. One of the largest

virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in Web Money and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, pleaded guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more pleaded guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.

There are a number of additional case studies available in this FATF reference paper.