ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Virtual Currency Business

Sector Specific AML/CFT Guidance Notes

October 2016

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 Unit, Enforcement Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road,
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000 Fax: 01624 646001
Website: www.iomfsa.im Email: aml@iomfsa.im

Contents

1. Foreword

For the purposes of this sector specific guidance, the term 'Virtual Currency Business' has the same meaning as paragraph (1) (1) (mm) of Schedule 4 to the Proceeds of Crime Act 2008 ("POCA") -

> (mm) the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies, including crypto-currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity.

By virtue of being included in Schedule 4 to POCA this sector is subject to the requirements of the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 ("the Code").

The Convertible Virtual Currency sector is included in Schedule 1 to the Designated Businesses (Registration and Oversight) Act 2015 which came into force in October 2015. This means that any person undertaking this business as defined must be registered with the IOMFSA prior to commencing business.

2. Introduction

The purpose of this document is to provide some guidance specifically for the virtual currency ("VC") sector. This sector specific guidance should be read in conjunction with the main body of the AML/CFT Handbook. It should be noted that guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

This document will cover unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the virtual currency sector and will provide further guidance in respect of customer due diligence ("CDD") measures where a once size fits all approach may not work. Also, some case studies are included to provide context to these unique risks. The information included in this document may be useful to relevant persons to assist with their risk assessment obligations under the Code.

This document is largely based on the 2014 FATF report *Virtual Currencies; Key Definitions and Potential AML/CFT Risks.*

The Authority recommends that relevant persons familiarise themselves with this, and other typology reports concerning the virtual currency sector.

The VC sector is a young and rapidly developing sector. It is therefore of utmost importance that relevant businesses keep up-to-date with typology reports and training.

3. Terminology

The terms virtual currency and digital currency are often used interchangeably however the two are very distinct.

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

Virtual currency is a narrower asset and is a digital representation of value which can be traded digitally. The nature of a virtual currency means that it does not need to be centrally controlled or administered. Virtual currency can be either convertible or non-convertible.

Convertible virtual currency, which includes crypto-currency, can be converted into a fiat currency, either directly, or through an exchange. For a currency to be convertible, there does not need to be set rate or an established benchmark, but that merely a market exists and the ownership rights can be transferred from one person to another, whether for consideration or not.

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 Schedule 4 to POCA definition does not extend to non-convertible currency businesses).

Fiat currency a.k.a. “real currency”, “real money” or “national currency” is the coin and paper money of a country that is designated as legal tender.

4. Inherent Product Risks

This section provides examples of risk factors that are inherent to the products and services offered by VC businesses. Inherent risks may be mitigated by putting into place effective controls. Such risks should be considered and factored into the business risk assessment as detailed in section 5 of this document.

4.1. Anonymity

1. Greater anonymity than traditional non-cash payment methods.
2. Traded on the internet, typically by non-face-to-face customer relationships.
3. May permit anonymous funding.
4. May also permit anonymous transfers if sender and recipient are not adequately identified.
5. Decentralised VC payment providers are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, functioning as accounts, may have no names or other customer identification attached, and the system has no central server or service provider.

6. The Bitcoin protocol does not require or provide identification and verification of participants, and the historical transaction records generated on the blockchain are not necessarily associated with real world identity.
7. The anonymity of many decentralised VC transactions limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity and presents a significant challenge to achieving effective AML/CFT compliance.
8. Decentralised VCs 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.
9. Software products have been developed to enhance decentralised VC's anonymity features, including coin mixers and IP address anonymisers. Use of these tools may make application of CDD measures nearly impossible.

Please refer to sections 7 and 8 of this document for details of how the above listed anonymity related inherent risk factors can impact on a relevant person and its ability to comply with the requirements of the Code.

4.2. Global reach and disaggregation

1. Services can be accessed via the internet (including via mobile phones) and can be used to make cross-border payments and funds transfers to and from anywhere, including high risk jurisdictions and potentially in breach of sanctions.
2. VCs commonly rely on complex infrastructures involving several entities, often spread across several countries, to transfers funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance, supervision and enforcement may be unclear.
3. Customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement, regulators and supervisors to access them.
4. This problem is exacerbated by the rapidly evolving nature of decentralised VC technology and business models, including the changes number of types and roles of participants providing VC payment services.
5. Components of a VC payment service may be located in jurisdictions that do not have adequate AML/CFT controls in general.
6. Decentralised convertible VCs, allowing anonymous person-to-person transactions, may seem to exist in a digital universe entirely outside the reach of any particular country.
7. Centralised VC payment service providers may be wilfully complicit in criminal activities as Liberty Reserve illustrates. See case study 6.1 for further details.

4.3. Other risk drivers

1. Near real-time settlement and irrevocability of transactions (no chargebacks).
2. Challenges in tracing the flow of VC and freezing or seizing illicit proceeds held in the form of VCs due to data encryption.

3. Lack of mechanism to delay, freeze or decline transactions to or from hosted addresses in the event of suspicious activity, court orders etc.
4. Even where risk based AML/CFT controls are in place, VC developers and providers may come from non-financial services backgrounds, where industry is not as highly regulated as the financial sector. As such, 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 VC is a new and developing industry.
5. Most jurisdictions do not have an existing AML/CFT framework for VC businesses and as such, Isle of Man VC businesses may be exposed to higher levels of risk by having customers, business partners or agents based outside of the Isle of Man.
6. High risk factors make VC payment services vulnerable to abuse by money launderers, terrorists, terrorist financiers and sanctions evaders.

5. Business Risk Assessment

Due to the nature of the rapidly evolving sector, the Authority expects that VC businesses should review and update their business risk assessment each time there is a new technological developments risk assessment or at least 6-monthly.

The general requirements of a business risk assessment are covered in section 3.1 of the AML/CFT Handbook. The below additional factors are of high importance to VC businesses and should be included in detail in the business risk assessment.

Inherent product risks -
The business risk assessment should include the full list of inherent risk factors listed in section 4 of this document with a note confirming which of the listed factors are applicable to the relevant person's business and why. For those that are applicable, there should also be a note detailing the steps taken and processes in place to mitigate the identified risk.

Application the AML/CFT requirements -
The business risk assessment should include the sub-headers listed under the application of AML/CFT requirements at section 5 of this document with a note confirming any difficulties the relevant person is likely to face in complying with the listed requirements and detailing the measures that have been put in place to combat each of these difficulties .

The relevant person will be expected to demonstrate to the Authority how it has been able to overcome such challenges in order to comply with the AML/CFT requirements. Instances in which the relevant person has not been able to comply with the AML/CFT requirements should be escalated to the Authority in a timely manner and must be formally documented in their annual compliance return

Examples of Code requirements and how the relevant person may find compliance challenging due to anonymity issues are detailed in section 7 of this document.

6. Customer Risk Assessment

The general requirements of a customer risk assessment are covered in section 3.3 of the AML/CFT Handbook. The below additional factors are relevant to the VC sector.

6.1. Higher risk indicators

As with all types of risk assessment, a holistic approach should be taken and the indicators below should be taken into consideration, together with all other relevant factors.

The customer -

1. is overly secretive or evasive about where the money is coming from, why they are using VC.
2. is using anonymiser software, a mixer or similar system to obscure the true identity of the remitter.
3. is actively avoiding personal contact without good reason.
4. is reluctant to provide or refuses to provide information, data and documents usually required in order to enable the transaction's execution.
5. provides false or counterfeited documentation .
6. 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.
7. is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals.
8. is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities.

The Source of Funds:

1. The transaction involves a disproportional amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.
2. The source of funds is unusual:
    a. third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation.
    b. funds received from or sent to a foreign country when there is no apparent connection between the country and the customer.
    c. funds received from or sent to high-risk countries.
3. There is an excessively high or low price attached to the VC 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.

4. Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the customer or the possible group of companies to which it belongs or other justifiable reasons.

7 Application of Code Requirements

The general requirements of a customer due diligence ("CDD") are covered in section 4 of the AML/CFT Handbook. The following sub-section aims to clarify how specific CDD requirements should be interpreted in relation to VC products and services.

7.1 Customer Due Diligence

7.1.1. Who is your customer?

"Customer" is defined in the Code as being the person –

(i) seeking to form a business relationship* or carry out an occasional transaction; or

(ii) carrying on a business relationship or carrying out an occasional transaction.

A customer can be a natural or legal person/arrangement. Paragraphs 10(3) (New business relationships), 11(3) (Continuing business relationships) and 12(3) (Occasional transactions) of the Code require the relevant person to identify the customer and verify the identity of the customer using reliable independent source documents.

It is important to establish whether the natural person who approaches your business is acting for a legal person/arrangement as the methods to comply with identification and verification ("ID&V") requirements are different for customers that are a legal person/arrangement than for those of natural persons. It may be more difficult for a VC business to establish this, particularly where the source of funds is from a numbered address rather than, for example, a bank account in the name of Mr X.

The relevant person should ensure that its customer take-on procedures include determining whether the customer is a legal person or arrangement. This should include asking the natural person who seeks to form the business relationship or carry out an occasional transaction to confirm whether they are acting in a personal capacity or on behalf of a legal person or arrangement. Ongoing monitoring of transactions should highlight as unusual activity transactions or patterns of transactions that are not in line with the expected activity of a natural person customer.

Methods to comply with ID&V requirements for natural persons and legal persons/arrangements are detailed at sections 4.5, 4.6, 4.7 and 4.8 of the AML/CFT Handbook.

*Please note that a business relationship will apply to certain types of business partnerships or other corporate arrangements in addition to traditional 'retail customers'.

7.1.2. Is your customer acting on behalf of another person?

Paragraph 13(2)(c) of the Code requires the relevant person to determine whether the customer is acting on behalf of another person and, if so, identify that other person, and take reasonable measures to verify their identity using relevant information obtained from a reliable independent source.

In order to determine whether the customer is acting for another person, the relevant person should consider:

1. who customer instructions come from;
2. the source of funds;
3. the destination of funds;
4. payment references or rationale that does not appear to relate to the purported customer; and
5. an unusual delay in answering questions (due to having to refer to a third party.

7.1.3. Source of funds

Paragraphs 10(3)(e) (New business relationships) and 12(3)(e) (Occasional transactions) require the relevant person to take reasonable measures to establish the source of funds. 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 should identify and verify the identity of this third party where necessary. It should also seek to establish the relationship between the customer and the third party and consider the rationale for the payment and whether this appears reasonable.

In the cases of a direct wire transfer or a cheque payment the source of funds is self-explanatory. There are instances where payments are made, such as by BACS, where the sender information is not ordinarily attached but is available upon request the business does not have to hold that information file, however must to be able to obtain it within 7 business days of a request from a competent authority.

Where the source of funds is a VC address (or similar numbered remitter), reasonable steps should be taken to determine the source of the virtual currency. Determining 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 what is known about the customer, then further investigation may be required to establish the source of the funds.

7.1.4. Beneficial ownership and control of a legal person/legal arrangement

Paragraph 13 of the Code (as detailed in section 4.3.4 of the AML/CFT Handbook) requires that the relevant person carry out CDD procedures in respect of the various parties who may own, control or direct the activities of a legal person or arrangement. For the relevant person to understand whether paragraph 13 applies in respect of a particular customer, it is essential to know if the customer is in fact a legal person or arrangement. See section 8.1.1 of this document for further guidance on determining the legal status of a customer.

Paragraph 13 of the Code (as detailed in section 4.3.4 of the AML/CFT Handbook) also requires the relevant person to identify and take a risk-based approach to verify the identity of the beneficiary of a payment or loans.

7.1.5. Politically exposed persons

Paragraph 14 of the Code (as detailed in section 4.15 of the AML/CFT Handbook) requires the relevant person to maintain appropriate controls for the purpose of determining whether a customer, its beneficial owners, controllers or known beneficiaries and to carry out the necessary additional CDD requirements for all foreign PEPs and any higher risk domestic PEPs.
Compliance with this paragraph may be impacted where –

- the relevant person has not identified their customer as a legal person/arrangement and therefore has not identified the beneficial owner(s) and controller(s) and is therefore unable to determine whether they are a PEP; or
- The real world identity name of known beneficiaries (i.e. VC address or equivalent) has not been obtained.

7.1.6. Identifying higher risk customers

Paragraph 15 of the Code (as detailed in section 4.3.6 of the AML/CFT Handbook) requires the relevant person to carry out enhanced due diligence procedures in relation to higher risk customers.

Paragraph 15(3) of the Code provides a list of matters that may pose a higher risk of ML/FT which includes activity in a List A (high risk) or List B (may be high risk) jurisdiction. The Authority considers “activity” to include transfers to or from third parties, meaning that the relevant person must know the geographical location of remitters and beneficiaries.

Where a transfer is made to or from a traditional bank account, it is possible to determine the geographical location of the account using an IBAN number or SWIFT reference but for decentralised VC transactions there is no central authority or branch. For VC transactions, the relevant person may take into account the user’s IP address but, as this only confirms the country or city where the internet was accessed (rather than residential address) and

due to the inherent anonymity related risks detailed in section 4.1 of this document, this should not be considered a reliable method in isolation.

7.2 Conducting appropriate scrutiny of transactions and forming a suspicion of ML/FT

Paragraph 9 of the Code (as detailed in section 3.4 of the AML/CFT Handbook) requires the relevant person to perform ongoing and effective monitoring of any business relationship which includes appropriate scrutiny of transactions. Particular attention must be paid to the scrutiny of unusual or suspicious activity.

Whilst transaction screening software designed to detect unusual values, volumes and patterns of transactions may be helpful, transactional patterns alone are unlikely to be considered sufficient grounds for suspicion.

Relevant persons are reminded of the criminal penalties for failing to report suspicions of ML/FT and of the potential impact of over-reporting as detailed in section 7 of the AML/CFT Handbook.

7.3 Record keeping

Paragraph 32 of the Code (as detailed in section 8.4 of the AML/CFT Handbook) requires the relevant person to keep records of CDD and such other records are sufficient to permit reconstructions of individual transactions and compliance with the Code.

The rationale for requiring transaction record is so that there is a clear audit trail of a transaction which may be used in the event of a ML/FT investigation to determine the source and destination of criminal or terrorist property that the authorities may seek to freeze, restrain or confiscate.

Failure to maintain appropriate records could potentially lead to a breach of the AML/CFT Code 2015, the Proceeds of Crime Act 2008 and the Anti-Terrorism and Crime Act 2003.

8. Case Studies

The examples below include some of the higher profile examples of where convertible virtual currency has assisted with Money Laundering and with Terrorist Financing. These examples have been taken from the FATF report – Virtual Currencies – key definitions and potential AML/CFT risks 2014:

8.1 Liberty Reserve

In what is to date the largest online money-laundering case in history, 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 (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

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was

arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

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 total sales price.

Silk Road achieved anonymity by operating on the hidden Tor 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, "sen[t] 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)

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, plead 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 plead 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.