ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Virtual Currency Business

Sector Specific AML/CFT Guidance Notes

May 2020

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
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

1. Foreword

For the purposes of this sector specific guidance, the term virtual currency business refers to a business conducting activity included in paragraph 2(6)(r) Schedule 4 to the Proceeds of Crime Act 2008 ("POCA"). The activity is defined as follows:

> **"Convertible virtual currency activity"** means 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, virtual assets or similar concepts where the concept is accepted by persons as a means of payment of goods or services, a unit of account, a store of value or a commodity;

By virtue of being included in Schedule 4 to POCA, a virtual currency business is subject to the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019. Also, this sector is included in the Designated Businesses (Registration and Oversight) Act 2015 which came into force in October 2015. The Financial Services Authority ("the Authority") has the power to oversee this sector for Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") purposes.

Any person looking to provide CVC activities in or from the Isle of Man should obtain relevant independent legal advice to ensure that the activities are subject to the appropriate regulatory framework i.e. whether the activity is designated business under the DBRO or could be licenceable under other legislation such as the Financial Services Act 2008.

2. Introduction

The purpose of this document is to provide some guidance specifically for the convertible virtual currency ("CVC") sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook"). It should be noted that although guidance is not law, it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

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 between sectors.

This document includes references to the following FATF documents:

- Guidance for a risk based approach - Virtual Assets and Virtual Asset Service Providers (June 2019);
- Guidance for a risk based approach – Virtual Currencies (June 2015); and
- 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. Also, some case studies are included to provide context to the risks of the sector.

2.1 National Risk Assessment

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

Considering the key risks and vulnerability of the sector, the CVC sector is rapidly evolving; it is also complex, the level of regulatory (and investigatory) expertise in the field is limited and it is a challenge to keep up with developments. Also, with these services there is a level of anonymity available which is greater than traditional non-cash methods and difficulty in linking an 'account' to a real identity. CVC providers should carefully consider features, products or services that potentially disguise transactions or hinder CDD and related measures.

A number of control measures have been put in place, however there are a number of ML and TF risks within the sector (some of which covered above) which cannot easily be mitigated. Therefore ML risk for CVCs in the IoM is assessed as medium high and the TF risk as medium.

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:

Convertible virtual currency (please see section 1 of this document for the Isle of Man definition of this term[1]), 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.

[1] It should be noted that FATF uses the term VASP to describe the sector, however in Isle of Man legislation the activity is defined as convertible virtual currency and expressly includes reference to "virtual asset".

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", "real money" or "national currency" is the coin and paper money of a country that 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 definition of CVC 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 representation of fiat currencies, securities, and other financial assets.

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. exchange between virtual assets and fiat currencies;
ii. exchange between one or more forms of virtual assets;
iii. transfer of virtual assets;
iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

2.3 Typical activity within the sector

By way of a breakdown of activity in the IoM, the three key types of registered CVC's typically undertake the following types of activity:

- **Administering, managing, lending, buying, selling, exchanging or otherwise trading** – allowing customers to exchange fiat currency for CVC and vice versa as well as trading between different CVC's.
- **Issuing, transmitting and transferring ("ICO") -** 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 discount early and for higher amounts purchased).
- **Providing safe custody or storage of CVC's -** customers can store or hold their tokens to pay for goods or services, typically referred to as a "wallet".

3. Risk Guidance

As demonstrated by the above examples, the CVC 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 CVCs enable non face-to-face business relationships. CVCs can also be used to quickly move funds globally and to facilitate a number of financial activities[2]. Factors such as this can indicate higher ML/TF 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 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:

- On-boarding / account opening;
- convertible virtual currency/virtual asset screening;
- the receipt of customer instructions;
- transactions into and out of customer account (or wallet);
- ongoing monitoring of the business relationship;
- technology / security issues where there is an online element to the business relationship; and;
- where any services are outsourced or delegated.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed under Part 3 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 cause it concerns, it should be determined whether this is suspicious or unusual activity. Please refer to Part 7 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 (Ongoing monitoring) of the Code:

[2] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

(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.

- 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 high 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;
- there is an excessively high or low price attached to the CVC 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 known 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 / 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; and
- 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 appropriate steps as explained in section 3 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- 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 enquires about how quickly they can end a business relationship where it is not expected;
- 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 or CVC which has a significant proportion of dark web activity;
- the customer is known to have criminal / civil / regulatory proceedings against him / her for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to the CVC sector. Further guidance surrounding the risk assessments is outlined in Part 3 of the Handbook.

A number of risk assessments must be carried out by sectors as set out in the Code, including:

- business risk assessments (paragraph 5);
- customer risk assessments (paragraph 6); and
- technological risk assessments (paragraph 7).

Due to the nature of the rapidly evolving sector, particular focus should be given to the technological risk assessment. This must estimate the risk of ML/FT posed by any technological developments, such as the use of online delivery channels and communication methods), to its business. The business risk assessment must also take into account the technology risk assessment.

3.3.1 Anonymity

The following list which is not exhaustive includes some factors to consider in relation to anonymity when undertaking CVC activity:

- It is associated with greater anonymity than traditional non-cash payment methods.
- Traded on the internet, typically by non-face-to-face customer relationships.
- May be used to facilitate anonymous funding.
- May also result in anonymous transfers if sender and recipient are not adequately identified.
- Decentralised CVC 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.
- A CVC protocol may not require a user to provide identification and verification, and the historical transaction records generated on the blockchain are not necessarily associated with real world identity.
- The anonymity of many decentralised CVC 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 CVCs 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 CVC's anonymity features, including coin mixers and IP address anonymisers. Use of these tools may make application of CDD measures nearly impossible.

3.3.2 Global reach and disaggregation

The following list which is not exhaustive includes some factors to consider in relation to the global reach of CVC 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 high risk jurisdictions; these payments could potentially be in breach of sanctions.
- Some CVCs 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 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.
- This problem is exacerbated by the rapidly evolving nature of decentralised CVC technology and business models, including the changes number of types and roles of participants providing CVC payment services.
- Components of a CVC payment service may be located in jurisdictions that do not have adequate AML/CFT controls.
- Decentralised convertible CVCs, allowing anonymous person-to-person transactions, may seem to exist in a digital universe entirely outside the reach of any particular jurisdiction.
- Centralised CVC payment service providers may be wilfully complicit in criminal activities as Liberty Reserve illustrates. See case study 6.1 for further details.

3.3.3 Other risk factors

The following list which is not exhaustive includes some factors to consider in relation to some other risk factors when undertaking CVC activity:

- Near real-time settlement and irrevocability of transactions (no chargebacks).
- Challenges in tracing the flow of CVC and freezing or seizing illicit proceeds held in the form of CVCs due to data encryption.
- Lack of mechanism to delay, freeze or decline transactions to or from hosted addresses in the event of suspicious activity, court orders etc.
- CVC 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 CVC sector is new and developing.
- Software updates or ‘forks’ bringing new technical features to a blockchain, consideration should be made if any such updates presents additional ML/TF risks.

- Many jurisdictions do not have an existing AML/CFT framework for CVC businesses and as such, IoM based CVC businesses may be exposed to higher levels of risk by having customers, business partners or agents based outside of this jurisdiction.
- High risk factors make CVC payment services vulnerable to abuse by money launderers, terrorists, terrorist financiers and sanctions evaders.

4. Customer due diligence

Part 4 of the Handbook[3] provides guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. It also provides general guidance on the timing of identification and verification of identity. Please also see the stand-alone guidance document in relation to source of funds and source of wealth. For details of particular concessions which may be relevant please see section 5 of this document and Part 6 of the Handbook. In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 9(9), 10(5), 12(11)) the procedures and controls must be provide that –

(a) the business relationship must proceed no further;
(b) the relevant person must consider terminating[4] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

4.1 Source of funds

Paragraph 8(3)(e) of the Code requires the taking of reasonable measure to establish the source of funds for all 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.

[3] At this time please see the stand-alone guidance document in relation to part 4 of the Handbook (customer due diligence) which is in use until the main body of the Handbook is fully updated.
[4] In relation to a New business relationship (paragraph 8) the business relationship must be terminated.

Please also see the stand-alone guidance document in relation to 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. 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 currency 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 must be undertaken to establish the source of the funds as per the requirements of the Code

4.2 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:

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 may include:

a) corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;
b) potentially tracing the customer's IP address; and
c) searching the Internet for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.[5]

5. Simplified customer due diligence measures

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

5.1 Exempted occasional transactions

Paragraph 11(5) of the Code (as detailed in part 6.5 of the Handbook) 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:

> **"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) (convertible virtual currency)** of Schedule 4 to the Proceeds of Crime Act 2008; or
>
> c) €15,000 in any other case;

Although verification of identity does not have to take place if the conditions are met, all other Code requirements under paragraphs 6 (customer risk assessment), 10 (continuing business

[5] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

relationships), 13 (beneficial ownership and control), 14 (politically exposed persons) and 15 (enhanced due diligence) continue to apply.

In order to reduce the compliance burden in relation to dealing with exempted occasional transactions, the Authority considers it acceptable in these circumstances for the relevant person to:

- complete a simplified customer risk assessment; and
- collect a reduced amount of identification information (lower or standard risk only)[6];

For exempted occasional transactions that pose a lower or standard risk of ML/FT and the relevant person has not identified any suspicious activity, relevant persons may accept a reduced amount of identification for natural persons.

This concession is typically used by CVC 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; and
- purchases a utility token within the exempted occasional transaction amount;

6. 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.

6.1 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

[6] Full name, date of birth and residential address could be obtained as a minimum in these circumstances.

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.

6.2. 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 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, “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 201. 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.

6.3. 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.