JUNE 2019

CRYPTO ASSETS: A SUMMARY OF FINANCIAL CRIME & REGULATION

KYT- CONSULTING
DIGITAL ASSET RISK CONSULTANCY

1

INTRODUCTION:

The current international and domestic legislation on combating financial crime is both strict and far reaching. It deals with a wide range of offences and offers guidelines on how to deal with funds and assets as well as how to handle client relationships. The digital market provides opportunities for individuals and businesses, both big and small, new ways to transact, invest and protect their money as well as raise capital. Unfortunately, this also gives opportunity to criminals.

This report will look at what theoretical issues arise from the digital market, where the current law aids in these issues and what may need to be done where it does not. We will also discuss possible future approaches and what the regulators are currently doing to stop possible exploitation.

02

THE ISSUES:

Theoretically, there are many ways in which criminals can exploit the digital market – Europol estimates that £3-4billion is laundered through crypto-assets in Europe each year. It is important for those interested in transacting/investing in the digital market, and those whose clients have a digital portfolio, to be aware of the risks posed.

It is worth noting that, as crypto markets are not currently under the remit of the FCA, users do not have access to the Financial Ombudsman Service nor the Financial Services Compensation Scheme.

As the use and popularity of the digital market grows, so does it's attention of the regulatory bodies. In 2018 the UK government established it's Cryptoassets Taskforce who have published a final report assessing the impact and potential harm of the market. The FCA have also released a consultation paper and, even in 2015, FATF themselves published guidelines to governments and the private sector regarding virtual or crypto currencies.

03

Segmentation of services means responsibility for supervision and enforcement is unclear

The recurring issues raised were the ease of online accessibility, the anonymity of both individuals and transactions as well as the globality of the network. It was first theorised that improper use would mainly result in online crime to buy illicit tools and services in criminal marketplaces, however, as the market matures, it is now understood that offline crime is just as common. Crypto assets that are convertible (or paired) with other crypto assets (such at Bitcoin & Ethereum) have therefore gained the most attention by the regulators due to their ability to convert into another cryptocurrency or fiat currency. This conversion, done many times over, can also conceal the origin of funds.

Other risks noted include, that many cryptocurrencies have no central server or administrative authority and many without any proper identification and verification protocols. This makes it hard to pinpoint the acting party who is laundering the funds and makes freezing/seizure of assets harder for law enforcement, especially if the servers span several jurisdictions. This also makes it unclear who holds the responsibilities for AML on the system, if there are any. Also, having the ability to have as many wallets as one wants, and the ease to create/delete them, increases anonymity.

The DEA in America have noted a steady decline in cash seizures, partly blaming this on Chinese Underground Banking Systems (CUBS). They believe there is a network where drug traffickers are using cash and Bitcoin to launder funds through over the counter exchanges were they have lax AML/KYC controls.

04

Wallet addresses have no names or any other customer identification attached in addition to the fact that they don't provide dividends, limiting any identifying papers trail even further

It has also been noted that there are special privacy crypto assets that aim to break the link between crypto transactions so they can't be traced through the Blockchain, as many of the larger crypto assets (by market capitalisation) can be, adding further challenges to this already opaque asset class.

Crypto wallet addresses have no names or any other customer identification attached in addition to the fact that they don't provide dividends, limiting any identifying paper trails even further. Furthermore, crypto assets commonly rely on complex infrastructures spread across several countries and jurisdictions. This segmentation of services means responsibility for supervision and enforcement is unclear. Centralised systems could potentially seek out countries with particularly weak AML/CTF regimes and Decentralised systems may exist entirely online and therefore outside the reach of any particular jurisdiction.

06

DEAR CEO

While the regulatory bodies have been keen to point out the risks posed by the new digital market, they have also recognised its benefits. Currently, the regulators would need to see tweaks and amendments to the current system before introducing it into the regulated market. However, given the most recent movements by the FCA and the Cryptoasset Taskforce, adoption may not be too far away here in the U.K.

The FCA in June 2018 sent out a 'Dear CEO' letter with best practice for banks who deal with crypto assets for financial crime prevention purposes. These were listed as:

- *Developing staff knowledge and expertise on crypto assets to help them identify the clients or activities which pose a high risk of financial crime*
- *Ensuring that existing financial crime frameworks adequately reflect the crypto related activities which the firm is involved in, and that they are capable of keeping pace with fast-moving developments*
- *Engaging with clients to understand the nature of their businesses and the risks they pose*
- *Carrying out due diligence on key individuals in the client business including consideration of any adverse intelligence*
- *In relation to clients offering forms of crypto-exchange services, assessing the adequacy of those clients' own due diligence arrangements*
- *For clients which are involved in ICOs, considering the issuance's investor-base, organisers, the functionality of tokens (including intended use) and the jurisdiction*

07

FINANCIAL ACTION TASK FORCE

The FATF Guidelines provide potential solutions to compliance challenges, providing technology-based theoretical solutions to the issues previously discussed and how crypto assets in a particular format could not only fit into the market but also provide a strong arm in the fight against financial crime and money laundering.

- *Application Programming Interfaces that provide customer ID info. or allow financial institutions to limit transaction size and velocity/pre-set conditions to be met before a transaction can be sent.*
- *New currencies could be built on different underlying protocols that can build-in risk mitigants or facilitate customer identification and transaction monitoring.*
- *3rd party digital identity systems to facilitate AML/CTF compliance.*
- *Development of business models/industry associations which provide a crypto asset or an individual with a "badge" to show they (or a specific transaction), has appropriate customer due diligence and has gone through appropriate monitoring.*

08 REGULATORY APPROACHES

The FATF Guidelines also show the regulatory approaches taken by an extensive list of countries. These include:

CANADA

They now treat persons/entities engaged in the business of dealing with crypto assets as money service businesses. It is expected that their obligations will be similar to existing MSB obligations which will include CDD, record keeping and an internal compliance regime as well as reporting suspicious and prescribed transactions.

HONG KONG

So far they have taken a cautious approach. Not seen as currency or securities per se, therefore, dealers/operators do not fall under MSB under AML/CTF policies unless involved in money changing or remittance services. However, they do have a statutory duty to report suspicious transactions to the Joint Financial Intelligence Unit and a failure to do so may amount to a criminal offence. The Regulator has reminded financial institutions to exercise caution and have extra vigilance when relationships deal with virtual commodities.

USA

Regulates any person/company engaged in acceptance/transmission of convertible cryptoassets and are subject to registration, customer id, record keeping and reporting requirements. Federal AML/CTF regulation covers both centralised and decentralised convertible cryptoassets and applies to a person acting on behalf of a 3rd party. 48 states regulate money transmitters and many are considering how law applies to cryptoassets E.g. New York Financial Services Dep. will shortly issue regulation requiring some virtual currency businesses to obtain a ‘bitlicence’ and comply with AML/CTF obligations, consumer disclosure rules, capital requirements and investment rules

09

CHINA

2013 released the Notice on Preventing Risks of Bitcoin. Required institutions which provide services including bitcoin registration, bitcoin wallet and bitcoin exchanging shall fulfil AML/CTF obligations and identify customers and record identification information. Also, enhanced monitoring measure on bitcoin service providers. Peoples Bank of China offices required to study Bitcoin related ML risks and take action to mitigate those risks.

FRANCE

Jan 2014: French Prudential Supervisory and Resolution Authority stated an entity engaged in intermediation with respect to purchase or sale of VC in exchange for fiat currency is a financial intermediary, who receives funds on a 3rd parties behalf, activities must be authorised and therefore subject to AML/CTF requirements. June 2014: published a report, intent to establish a framework to deter the use of VC for fraud and ML.

GERMANY

Qualifies Bitcoin as financial instruments but are not denominated legal tender. No requirement for licence for commercial activities, mining and buying/selling of mined bitcoin. Authorisation requirement may arise if additional factors: if traded via internet platforms, investment broking, multilateral trading facility, exchange bureaus that offer to change legal currencies directly into Bitcoin. Generally at the moment decide on a case-by-case basis when receiving enquiries as to whether they need a licence.

10

ITALY

Not considered legal tender. Jan 2015: issued warning on use of virtual currencies and endorsed the EBA 'opinion' on VC.

RUSSIA

Issuing monetary surrogates is prohibited in the Russian Federation "Art 27 of Federal Law On the Central Bank of the Russian Federation". Bank of Russia warns individuals, legal entities and primarily credit/non-credit institutions against use of VC for goods, services or real currency (Rubles or foreign currency). Due to anonymous nature of the issue of VC by an unlimited number of persons, individuals may unwittingly becoming involved in illegal activities including ML/TF. Ministry of Finance jointly with Bank of Russia developed draft law imposing a ban on electronic monetary surrogates and electronic monetary surrogates transactions.

SINGAPORE

March 2014: Monetary Authority of Singapore announced it will regulate VC intermediaries operating in Singapore to address potential ML/TF risks. Regulations requiring VC intermediaries to verify customer identity and report suspicious transactions.

SOUTH AFRICA

Issued a user alert in September 2014 to be aware of risks associated with VC. Currently no specific laws or regulations that address use of VC. Cannot be used commercially.

10

SWITZERLAND

June 2014: The Swiss government published a study which declared that Professional trade in VC and operation of trading platforms in Switzerland generally come under the scope of the Anti Money Laundering Act. Required to comply with obligation to verify identity of contracting party and establish party of beneficial owner. Purchase and sale of VC and operation of trading platforms also come under AML act. Convertible VC can facilitate anonymity and cross-border asset transfers – heightened ML/TF risks – strict CDD and client ID and require a banking licence.

EUROPEAN BANKING AUTHORITY OPINION

Long term regulatory approach would require substantial body of regulation and would need to comprise governance requirements of several market participants, segregation of client accounts, capital requirements that are accountable for integrity of a virtual currencies scheme and its key components, including its protocol and transaction ledger. Short term – make financial institutions aware of risks and discourage buying, holding or selling virtual currencies. Declare virtual currency exchanges as ‘obliged entities’ that must comply with AML/CTF policies.

11 PREVIOUS CASES:

LIBERTY RESERVE

Described as the largest online money laundering case in history, this Costa Rica based money transmitter and 7 of its principals and employees were charged with operating an unregistered money transmitter business and laundering more then $6 billion in illicit proceeds. It had more than 55 million users worldwide and used its own currency, Liberty Dollars, but at each end transfers were denominated and stored in fiat currency.

SILK ROAD

A hidden online website designed to enable its users to buy and sell illegal drugs, weapons, stolen id information and other stolen goods and services. The US Justice Department seized 173,991 Bitcoins worth more than $33.6million at the time of seizure from seized computer hardware. They had their own hidden network and currency, their own escrow account and accepted Bitcoin exclusively as participants could easily hide identity.

WESTERN EXPRESS INTERNATIONAL

Multinational, internet-based cybercrime group. They used a series of anonymous chat/email accounts and virtual currency accounts to conceal the existence and purpose of the criminal enterprise. They took payment mainly in e-Gold and WebMoney for stolen id information to use for further frauds.

12 OTHER CASES:

The Financial Crime Enforcement Network penalised a California-based cryptocurrency trader for violating the BSA's registration and reporting requirements. Eric Powers conducted an unregistered peer-to-peer exchange which is required by US law to observe the AML program regarding money transmitters. Accused of processing numerous suspicious transactions – many to the Silk Road network – without raising a suspicious activity report.

New York State also conducted its first conviction, this time for crypto money laundering. The Manhattan District Attorney's Office named two individuals who laundered $2.8 million through sales of steroids and other drugs via their website and on the dark web. Bitcoin payments were laundered through intermediary wallets and then converted to US dollars using an exchange platform. In addition to crypto, the defendants accepted fiat currency via Western Union which they then laundered through false identities or international wire transfers from receivers outside the US.

FinCEN assessed a $110million civil penalty against BTC-e for willfully violating U.S. anti-money laundering laws. It was a foreign MSB operating on American soil and handled Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. It handled transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking

Police in Spain shut down a "Crime-as-a-service" (CAS) enterprise. Wallets containing 9 million euros were also frozen. Besides the bitcoin wallets, which were frozen, two bitcoin ATMs and cash totalling nearly 17,000 euros were seized in addition to 11 cars, computers, devices, and other properties. Europol also stated that Spanish Authorities froze four cold wallets and 20 hot wallets, to which €9 million was transferred, as well as several bank accounts.

13

ABOUT KYT CONSULTING

You have the competencies in your profession. The terms proof of funds, anti-money laundering, safe custody and settlement are all a part of daily business. However, Blockchain creates new challenges. The way assets are transferred, stored and recorded are all changing.

KYT Consulting is a Digital Asset Risk Consultancy, helping to mitigate the risks associated with handling Digital/Crypto Assets. Focusing on the Legal, Accountancy & Finance Sectors, our consultants provide considerations for best practice whilst advising on cases involving Digital Assets.

KYT Learning & Development provides learning and development, focusing on Blockchain technology and Digital Assets, formed to enable client facing Professionals to have better, more informed, conversations with clients and identify opportunities that exist in this complex landscape.

To learn more about our consultancy services:

www.kyt-consulting.com/consultancy

To learn more about our Learning & Development options:

www.kyt-consulting.com/learning

For general enquiries:

info@kyt-consulting.com
+44 (0)207 097 3817