RUDICH

Safeguarding Financial Integrity

.Consultation on the Transposition of 5MLD
Sanctions and Illicit Finance Team
HM Treasury
1 Horse Guards Road London
SW1A 2HQ
London

10 June 2019

Dear Sir/Madame,

Re: Consultation on the Transposition of 5MLD

Please accept this as a response to the request made during the HM Tresury's (HMT) meeting on the *Consultation on the Transposition of the 5AMLD: regulation of cryptoassets* held on 10 May 2019. This document specifically refers to the section on cryptoassets only but would be happy to discuss other aspects of the transposition of the 5AMLD separately if your team wishes to do so.

This is a submission on behalf of Rudich Advisory.

About Rudich Advisory

Rudich Advisory is a strategic advisory firm that offers tailor-made services in financial crime prevention to safeguard the integrity of the global financial system. Clients range from traditional top tier financial institutions, to regulators, non-for-profit organizations, emerging technology companies and industry bodies. Its founder, Denisse Rudich, is a financial crime prevention specialist who is involved in a number of global initiatives to build collaboration to fight financial crime. Amongst others, these include acting as a member of the Global Coalition to Fight Financial Crime launched by the World Economic Forum and Europol, setting up the AML/CFT Working Group for a global crypto/virtual assets industry body, and as the Director of the G7/G20 Research Groups (London).

Response to Consultation

Reference: *Box 2.C: Cryptoassets*

12. 5MLD defines virtual currencies as "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach.

The Governments approach to regulating exchange and utility tokens is appropriate but care should be taken to define which types of utility tokens should be subject to regulation. For example, many utility tokens serve to provide access by individuals to a service, physical or (in some cases) virtual product offered by a specific provider. This is similar to Sainsbury's loyalty points that can then be used in lieu of cash to buy groceries or a Starbucks loyalty programme. The challenge in regulating utility tokens in and off themselves would be that of how do you

limit what you regulate? Would the Government regulate a coffee provider that is using blockchain technology for traceability purposes and also offering tokens to its customers in exchange for buying coffee from it as a sole supplier and accepting agent of that token? What are the money laundering and terrorist financing risks in that situation?

Where the government definitely should play a role is:

- Where a token becomes tradeable on an exchange or accepted as a means of "payment" / transfer of value by more than 1 agent; or
- Where a token could be loaded onto finance products, such as credit card services offered by Wirex, and be used as a means of exchange, payment or have an accrued value.

This would then cover the activity of companies such as Ethereum & Ripple who issued a token to allow users to use its protocol but whose tokens then became tradeable on secondary markets.

The question then becomes: should the government regulate the token type or the service provider that allows for the token to be used in a manner similar to a financial instrument?

Is the 5MLD definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there assets likely to be considered a virtual currency or cryptoasset which falls within the 5MLD definition, but not within the Taskforce's framework?

The one area that may need to be covered is the **issuance** of crypto/virtual assets that is not included here and would be needed to allow the government to regulate Initial Coin Offerings (ICOs). Also, due to the global nature of virtual assets, consideration should also be given to aligning as close as possible to the Financial Action Task Force (FATF) definition included here:

> *A virtual asset is 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 that are already covered elsewhere in the FATF Recommendations.*[1]

Recommend amending definition to the following:

"a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange, ***payment or investment purposes*** *and which can be* ***issued,*** *transferred, stored and traded electronically.*"

Also, care should be taken with regards to mentioning "cryptography" or "blockchain" as new technological layers or technology could emerge that would not be captured by the law oe regulation.

13. 5MLD defines a custodian wallet provider as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual

[1] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

currencies". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the 5MLD definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there wallet services or service providers likely to be considered as such which fall outside the 5MLD definition, but should come within the UK's regime?

The government should look to the work completed by the Australian regulator on virtual wallets. It is also recommended that the Government align language to FATF definition; rather than labelling them "virtual currencies," consideration should be given to calling them "virtual assets" as not all tokens would necessarily be considered to meet the definition of a "virtual currency."

Different types of wallets exist, including: online, mobile, desktop, hardware and paper wallets and new types appear to be emerging.

The following article provides a dated if useful description of the different wallet types available: https://medium.com/@fastinvest/the-most-comprehensive-cryptocurrency-wallet-guide-5e820a26ed44

The risks associated for each type of wallet as well as the different protocols and technology that could be used to increase ML/TF risk (i.e. Darkwallet 2.0[2]) should be contemplated as part of the determination of whether the format in which the wallet is available should also be taken into consideration.

14 Should the FCA be assigned the role of supervisor of cryptoasset exchanges and custodian wallet providers? If not, then which organisation should be assigned this role?

Absolutely with the caveat that the FCA should be given the right additional resources (people, training and technological tools) to be able to properly understand the industry it is regulating and to properly monitor and support the industry in managing risks posed to the integrity of the global financial system.

15 The government would welcome views on the scale and extent of illicit activity risks around cryptoassets. Are there any additional sources of risks, or types of illicit activity, that this consultation has not identified?

The latest public statistic available was issued by Europol in early 2018, where it highlighted that approximately EUR 3-4million was laundered through crypto assets, including through dark web transactions, fraudulent ICOs, hacks on exchanges and sanctions evasion.[3] As with most statistics related to financial crime, there is a large variance associated with this number. What is clear is that as virtual assets become more widely adopted, there is an upward trend in criminal abuse of this technology. Europol is likely to have some of the latest statistics.

[2] See: https://www.coindesk.com/this-binance-backed-crypto-startup-wants-to-anonymize-everything
[3] www.bbc.co.uk/news/technology-43025787

16 The government would welcome views on whether cryptoasset ATMs should be required to fulfil AML/CTF obligations on their customers, as set out in the regulations. If so, at what point should they be required to do this? For example, before an 'occasional transaction' is carried out? Should there be a value threshold for conducting CDD checks? If so, what should this threshold be?

ATMs are definitely vehicles that are being used for laundering the proceeds of crime. Elliptic presented a study at the Europol C3 Conference that it worked on with the London Metropolitan Police that may be worthwhile looking into.

As wider adoption occurs, the business case for these types of ATMs will grow and the Government should seek to strike a balance between stifling business growth and managing AML/CFT risk. It is therefore recommended that the same threshold that applies to MSB transactions is applied to deposit/withdrawal of virtual assets ATMs to guard against anti-industry sentiments but, from a data protection perspective, to require that the amount of personal data that is shared with these ATM providers is not excessive / is proportionate to identified risk.

17 The government would welcome views on whether firms offering exchange services between cryptoassets (including value transactions, such as Bitcoin-to-Bitcoin exchange), in addition to those offering exchange services between cryptoassets and fiat currencies, should be required to fulfil AML/CTF obligations on their customers.

Absolutely. Crypto-to-crypto exchanges offer a way for money to be layered and sent across borders instantaneously. The Government should consider bringing into scope the following virtual assets service providers:[4]

- Crypto Lending Apps
- Crypto Credit Cards
- Crypto Payment Apps
- Centralized Crypto Exchanges
- Crypto Derivatives Trading Platforms
- Crypto Brokers
- Crypto OTC Desks
- ICO Issuers
- Crypto Funds
- Crypto Custodian Wallet Providers
- Crypto Investment App

18 The government would welcome views on whether firms facilitating peer-to-peer exchange services should be required to fulfil AML/CTF obligations on their users, as set out in the regulations. If so, which kinds of peer-to-peer exchange services should be required to do so?

This is a question that appears to be linked to the debate on whether and how to regulate decentralized (DEX) exchanges. The only comment is that it will be very difficult to do so given

[4] Sourced from survey conducted by GDF available at: https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf

the supranational nature of some of these exchanges and that the assets linked to these types of exchanges are in cold wallets, some of which are kept offline. The Government may wish to consider working in a multilateral way with other countries to address DEX and peer-to-peer exchanges.

19 The government would welcome views on whether the publication of open-source software should be subject to CDD requirements. If so, under which circumstances should these activities be subject to these requirements? If so, in what circumstances should the legislation deem software users be deemed a customer, or to be entering into a business relationship, with the publisher?

The publication of open-source software should not itself be subject to CDD requirements. Doing so would likely have a negative impact on innovation, could create a poor precedent for all software developers to KYC their customers and leads to a situation that would generate barriers to access for legitimate means. That said, the Government should consider utilizing cybercrime detection tools, partnering with organizations such as Cyber Alliance or initiatives such as Tech Against Terrorism to develop ways to identify and monitor open source protocols or software that has been developed for nefarious means or that could be used to support criminal behaviour (i.e. mimblewimble or mixers/tumblers) and consider appropriate measures.

20 The government would welcome views on whether firms involved in the issuance of new cryptoassets through Initial Coin Offerings or other distribution mechanisms should be required to fulfil AML/CTF obligations on their customers (i.e. token purchasers), as set out in the regulations.

Any Initial Coin Offerings (ICO) that targets consumers and is linked to raising capital should be subject to a) registration and b) be required to meet AML/CTF obligations. A marker that could be used by the UK Government could be similar to that used by the SEC after their Chairman explained that tokens that "feature and market the potential for profits based on the entrepreneurial or managerial efforts of others contain the hallmarks of a security under U.S. law."[5]

It is estimated that over USD7billion was raised in 2017 with a study citing that over 85% were fraudulent. So in addition to AML/CFT measures, there should be a strong consumer awareness campaign to protect the retail market.

21 How much would it cost for cryptoasset service providers to implement these requirements (including carrying out CDD checks, training costs for staff, and risk assessment costs)? Would this differ for different sorts of providers?

On average, it takes a start-up between 6 to 12 months to set up an AML/CFT framework covering: risk assessment, CDD/KYC, monitoring, training and awareness, SAR reporting and

[5] https://www.sec.gov/ICO

record-keeping. Cost would be dependent on size of customer base, geographic regions of operation, and the ability to get suitably skilled persons to develop effective frameworks.

Establishing this requires specialist, often expensive resource (between £600-£1200 day rate) plus additional cost of technological tools and products to allow for effective implementation.

Costs would be similar to other providers subject to AML/CFT that operate on a global scale (smaller banks, emerging FinTechs, MSBs or gaming industry).

22 To what extent are firms expected to be covered by the regulations already conducting due diligence in line with the new requirements that will apply to them? Where applicable, how are firms conducting these due diligence checks, ongoing monitoring processes, and conducting suspicious activity reporting?

There is definitely a desire for virtual assets firms that will be subject to regulation to have AML/CFT regulation in place and some more established firms have a certain level of AML/CFT measures in place. However, some apply fairly basic CDD/KYC measures and adopt financial thresholds to determine different levels of due diligence (simplified vs. enhanced documentary requirements) as opposed to basic due diligence levels based on AML/CFT risk. There is a definite need for the industry as a whole to understand the AML/CFT risks associated with different products and services associated with virtual assets.

Those that have AML/CFT measures in place are or have adopted similar technological solutions to emerging FinTechs, such as selfie matching, biometric authentication, real time verification of ID, etc. but are also promoting the use of blockchain for KYC/KYB solutions.

The key area were non-'traditional' AML/CFT measures are needed is related to transaction monitoring. This type of activity require different tools, such as Chainalysis or Elliptic, to monitor crypto-to-crypto transactions and existing tools to monitor crypto-to-fiat once a virtual asset has been transferred to fiat.

23 How many firms providing cryptoasset exchange or custody services are based in the UK? How many firms provide a combination of some of these services?

That is a bit of an unknown at the moment but the UK definitely provides thought leadership in this space.

24 The global, borderless nature of cryptoassets (and the associated services outlined above) raise various cross-border concerns regarding their illicit abuse, including around regulatory arbitrage itself. How concerned should the government be about these risks, and how could the government effectively address these risks?

Consideration should be given to the model that has been adopted for other firms marketing services to UK consumers. Similar to the gaming industry, the UK could offer online operators UK licenses to allow them to provide online facilities to UK residents. This would not fully address the risk of online overseas service providers offering services but could act as a deterrent.

With regards to regulatory arbitrage, the best that the UK maybe be able to do is promote the adoption of AML/CFT measures via FATF and FATF style regional bodies and support local implementation of these measures as this is a very real risk.

25 What approach, if any, should the government take to addressing the risks posed by "privacy coins"? What is the scale and extent of the risks posed by privacy coins? Are they a high-risk factor in all cases? How should CDD obligations apply when a privacy coin is involved?

With regards to privacy coins, the key difference between these and traditional virtual assets is the inability to trace the coin using new technological tools due to privacy-preserving software. However, it is essential that as new privacy coins emerge, that the Government understand what data transfer requirements are built into these coins as well as the risks posed by privacy-preserving features that are included. A product risk assessment or an exercise along those lines would be a way to identify and develop ways to manage risks.

Once AML/CFT measures are adopted, depending on the type of protocol and exchange used, the service provider should be able to verify the identity of the privacy coin holder and should know the volume of coins/value contained in the wallet linked to a particular user's account. In the absence of AML/CFT regulation world-wide, it would be prudent to treat privacy preserving coins as presenting a higher risk of money laundering.

CDD should apply via the relevant virtual asset service provider, and consideration given to including identification of source of funds/wealth provision as an enhanced due diligence measure.