30 May 2019

To: HM Treasury

Re: Consultation on 5AMLD

To whom it may concern:

We are writing in response to HM Treasury's *Transposition of the Fifth Money Laundering Directive: Consultation* document published on 15 April 2019. Our response focuses on topics and questions the consultation poses on cryptoassets.

As the leading UK-based provider of blockchain monitoring and AML compliance solutions for the cryptoasset industry, we welcome the government's progress in developing a clear and effective domestic cryptoasset regulatory framework, and applaud its engagement with the private sector. In particular, we believe that the government's forward-looking approach for a regulatory framework that extends beyond the basic requirements of 5AMLD is a prudent one - though we offer views on the feasibility and advisability of certain specific issues that any such expansion of the UK's regulatory framework should consider.

In compiling our response, we've drawn from our ongoing interactions with cryptoasset business located in the UK, and beyond, as well as from our research and analysis of cryptoasset blockchains. Across April and May 2019 we engaged in numerous discussions on 5AMLD, including an industry briefing event we hosted on 16 April, to obtain input and views from our customers and other industry participants on matters related to the government's consultation.

We look forward to continuing our engagement with you on 5AMLD and other cryptoasset initiatives. At Elliptic, it is our mission to ensure that the UK is a safe environment for the trusted delivery of innovative cryptoasset services, and we plan to continue working with our customers and industry partners to that end.

Please do not hesitate to contact us if you have any specific questions regarding our response.

Sincerely,

David Carlisle
Head of Community, Elliptic
London, UK

Response to the Consultation

Please note that we have not responded to every question the government posed in the consultation but address select questions as indicated below.

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 transparency of many cryptoasset blockchains, or public ledgers, makes it possible to analyse macro-level information about the flow of illicit funds between entities in cryptoasset ecosystems. Determining the exact level of illicit activity that occurs using cryptoassets faces a number of methodological challenges - but with an overall estimated global market value of as much as $200 billion[1], it is likely that global illicit funds flows involving cryptoassets are in the low billions, as a minimum. Last year, Europol estimated that cryptoasset-related laundering figures might total as much as £4 billion.[2] The US Treasury estimated that in 2018 alone the total value of cryptoassets stolen through theft and hacks was $1.5 billion.[3]

At Elliptic, we conducted a study in January 2018 that examined the flow of funds between known illicit entities in the bitcoin ecosystem and known bitcoin conversion services, such as exchanges, bitcoin ATMs, mixers, and others.[4] The study did not attempt to identify all illicit activity occuring in the bitcoin network but rather examined patterns of funds flows through conversion services involving illicit source or destination addresses. The study had three key findings:

[1] See: https://coinmarketcap.com/
[2] See: https://cryptocoremedia.com/europol-crime-crypto/
[3] See: https://home.treasury.gov/news/press-releases/sm687
[4] See: https://www.elliptic.co/white-papers-and-reports/fdd-bitcoin-laundering

- 1) Illicit funds comprised a small proportion of overall bitcoin flows through conversion services. Only 0.67% of overall funds flows through bitcoin exchanges and other conversion services involved funds from illicit sources.
- 2) Illicit funds passed overwhelmingly though conversion services located in Europe, which we hypothesised was the result of criminals targeting cryptoasset services that they knew to be unregulated. In 2016, for example, nearly 57% of all identified global illicit bitcoin funds flows that passed through exchange platforms went through exchanges in Europe. The proportion of funds flows through the US, which issued guidance in 2013 clarifying that cryptoasset businesses must apply AML/CTF controls, was far smaller. We therefore identified a correlation between the presence of regulatory frameworks and the prevalence of money laundering using bitcoin.
- 3) The proportion of illicit funds passing through bitcoin exchange services as a percentage of all funds flows worldwide decreased over the period from 2014 - 2016. We surmise this is due to the growth in the number of legitimate users of bitcoin over time, as well as the application of AML/CTF controls at many large exchanges.

These findings are important. They suggest that the sometimes popular notion that all cryptoassest activity is illegal is flawed; but they underscore that the implementation of 5AMLD is a welcome step given that some European cryptoasset businesses appear to have provided a significant unregulated gap for illicit financial flows.

The government's consultation notes that in addition to money laundering and terrorist financing, other crimes that cryptoassets can facilitate include fraud, scams, and cybercrime. We agree with this assessment. Since we conducted the study described above, we have continuously monitored trends in the illicit cryptoasset typologies. We observe several trends of illicit activity in cryptoassets, including:

- *Increasing complexity of money laundering and terrorist financing typologies:* The expansion in the availability of new, innovative cryptoasset products and services has resulted in new platforms that criminals can exploit. Increasingly, typologies we observe involve criminals utilising numerous cryptoasset product and service types, with funds moving across various cryptoasset platforms throughout the money laundering process - adding challenges to detection and analysis.

  Generally speaking, terrorist financing with cryptoassets remains confined to a small number of isolated cases, but our recent analysis suggests that terrorist financiers have also begun to deploy more sophisticated methods of utilising cryptoasset addresses in an attempt to obscure funds flows.

- *More widespread use among criminal actor types and predicate offenses:* Cybercrime (including hacks and ransomware), and dark web market activity continue to account for an overwhelming proportion of criminal activity using cryptoassets. However, in recent months and years we have seen the range of

illicit actors using cryptoassets expand to include a broader and more diverse array of actors, including more traditional organised crime groups involved in narcotics trafficking, human trafficking, tax evasion, and other crimes.

- *Increased privacy coin usage:* The public and transparent nature of many cryptocurrency blockchains, such as those found in bitcoin, ethereum, and others, makes it possible to perform forensic analysis on illicit flows, and for cryptoasset companies to monitor customer activity for signs of risks using tools such as those we provide at Elliptic. A substantial amount of global cryptoasset trading and transaction volume occurs in these highly transparent coins. Despite the proliferation in the number of cryptoassets available, bitcoin still comprises more than 50% of all cryptocurrency trading volume, and it remains by far the most widely used cryptoasset for criminal purposes. However, recently we have seen evidence of criminals increasingly relying on privacy coins to raise funds and to facilitate the money laundering process. We comment further on privacy coins in relation to question 25 below.

One financial crime risk the government does not mention in its consultation relates to sanctions evasion.

Among the most significant recent illicit finance trends we have observed is the emergence of state actors into the cryptoasset space.[5] Our research, as well as public information supplied by research institutions[6] and both intergovernmental and governmental sources[7], suggests that countries such as Iran and North Korea are now accessing cryptocurrencies at significant volumes, potentially in the tens or even hundreds of millions of dollars. Our own research indicates that in a single instance in the summer of 2018, North Korean-linked cybercriminals were able to convert bitcoin totalling approximately $13 million that they stole from a South Korean exchange.[8]

This type of activity has important implications for sanctions compliance. In the US, the Department of the Treasury's Office of Foreign Assets Control (OFAC) has undertaken a number of recent measures to clarify how activities involving cryptoassets are implicated by sanctions measures.[9]

---

[5] See: https://www.elliptic.co/our-thinking/cryptocurrency-exploitation-nation-states
[6] See: https://rusi.org/publication/occasional-papers/closing-crypto-gap-guidance-countering-north-korean-cryptocurrency
[7] See: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf
[8] See: https://www.elliptic.co/our-thinking/following-money-from-bithumb-hack
[9] See: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs; https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13827.pdf; https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf;https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf; https://home.treasury.gov/news/press-releases/sm556

Our interactions with our customers in the US suggest that OFAC's actions in this space have provided important initial clarity for cryptoasset businesses regarding the extent and nature of their US sanctions obligations.

We therefore recommend that, separate to the 5AMLD consultation, HM Treasury's Office of Financial Sanctions Implementation should provide clarification on firms' UK sanctions compliance obligations where cryptoassets are involved. We recently released a report to assist cryptoasset businesses in managing sanctions-related risks, and we would welcome further engagement between the government and private sector on this important topic.[10]

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?

Cryptoasset ATMs should be subject to AML/CTF requirements.

Cryptoasset ATMs are a compelling innovation that play an increasingly important role in the cryptocurrency ecosystem. They provide a reliable method for rapidly transferring cryptoassets into fiat, or vice versa. They offer a useful avenue for moving cash from one counterparty to a cryptocurrency wallet belonging to another person located elsewhere - and as such, some industry participants view them as playing a critical role in furthering financial inclusion and broader cryptoasset adoption. Available information suggests that as of May 2019 there are as many as 234 cryptoasset ATMs located across the UK[11], and over 800 located across Europe.[12]

However, because they enable cash-loading, cryptoasset ATMs can provide an attractive platform for money laundering, and especially for money mule activity. Open source reporting cites Europol cases that have linked cryptoasset ATMs in Europe to major money laundering operations by international narcotics traffickers.[13] Cryptoasset ATMs have also featured in cases of fraud, in which criminals posing as tax collectors or other public officials convince victims to deposit cash funds in cryptoasset ATMs for onward transfer to wallets controlled by the fraudsters..[14]

[10] See: https://www.elliptic.co/white-papers-and-reports/sanctions-compliance-cryptocurrency-guide
[11] See: https://coinatmradar.com/country/225/bitcoin-atm-united-kingdom/
[12] See: https://coinatmradar.com
[13] See: https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/
[14] See: https://www.newsbtc.com/2018/10/05/scammers-use-cryptocurrency-atms-to-target-potentially-vulnerable-victims/

Regulating cryptoasset ATMs would close this gap significantly. Elliptic counts among its customers some of the largest providers of cryptoasset ATM services globally, and we have observed how cryptoasset ATM providers can successfully comply with regulation. Our customers include cryptoasset ATM businesses in the US that apply our transaction monitoring solutions, as well as other AML/CTF controls, and have successfully acquired licenses in multiple US states.

Because cryptoasset ATMs can provide an attractive method for laundering cash proceeds using 'money mule' techniques, a value-agnostic approach that requires cryptoasset ATMs to apply AML/CTF measures to all customers, regardless of transaction values, could act as a powerful control against money muling risks among this segment of service providers. One of our cryptoasset ATM customers has indicated to us that among the most important AML controls it has instituted is a requirement that all customers provide KYC information prior to transacting, regardless of transaction value or volume.

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.

We believe strongly that the government should bring firms offering exchange services between cryptoassets (or 'crypto-to-crypto exchange services') within the regulatory scope. The omission of crypto-to-crypto exchange platforms from the scope of 5AMLD is one that presents a significant gap in EU-wide efforts to mitigate cryptoasset risks.

As the government's consultation paper notes, the underlying premise for focusing regulation on crypto-to-fiat exchanges is that criminals usually must 'cash out' their illicit cryptoasset proceeds by converting them to fiat currencies that are easier to spend and utilise for practical purposes. This approach was advocated by the FATF's 2015 guidance on virtual currencies.[15]

Since then, criminal typologies and money laundering methodologies in the cryptoasset space have evolved significantly. As the cryptoasset ecosystem has grown, it has become possible for users to trade among numerous cryptoassets and conduct activities *within cryptoasset ecosystems* with greater ease.

For example, consider the following scenario:

- 1) A cybercriminal network obtains bitcoin after hacking a bitcoin exchange.

[15] See: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

- 2) The cybercriminal network transfers the stolen bitcoin from its own wallet to a crypto-to-crypto exchange service, where it purchases another cryptoasset.
- 3) The cybercriminal network uses the cryptoasset to purchase goods and services from vendors that accept cryptoassets as a form of payment.

Under 5AMLD, none of this activity would be regulated for AML/CTF purposes. Even if at stage 3 the criminal had chosen to cash out at a fiat-to-crypto exchange service, the crypto-to-crypto activity at stage 2 would still be conducted without KYC having been applied, allowing the criminal network to integrate funds into the financial system free of oversight at a critical stage in the money laundering process.

One example of crypto-to-crypto exchange activity facilitating money laundering is in the case of the WannaCry ransomware attack of May 2017. In that instance, the North Korea-linked Lazarus Group of cybercriminals exchanged bitcoin derived from the cyber attack worth approximately $144,000 for the privacy coin monero at the Shapeshift coin-swap platform registered in Switzerland. Blockchain analytics enable us to trace of the acquired bitcoin from the criminals' wallets to the point of their exchange at Shapeshift; however, once they are converted to monero, traceability becomes impossible.

Where this activity sits outside the regulatory perimeter, it presents a significant risk that criminals can swap cryptoassets without AML/CTF measures being applied - allowing criminals to operate with a high degree of anonymity.

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?

Peer-to-peer (P2P) exchange services play an important role in cryptoasset ecosystems. Where large, centralised exchange platforms conduct activity in a manner that resembles that of more traditional financial intermediaries, P2P exchange services allow users to interact and swap cryptoassets directly. P2P exchange services can take a number of forms, including:

- *individual P2P exchangers* - people who make it their business to facilitate and broker trades between other cryptoasset users, whether fiat-to-crypto, or crypto-to-crypto;
- *advertising websites/boards* - individuals can post their desire to trade cryptoassets on any website or online message board; under these circumstances, the website or board administrator has no role in the transfer of funds but merely acts as a site on which people can indicate their desire to trade;
- *P2P exchange platforms* - this includes dedicated platform sites such as LocalBitcoins, Paxful, and other services that allow cryptoasset traders to seek out other traders; individual P2P exchanges may also advertise their services on

these platforms; unlike simple websites which are entirely uninvolved in the cryptoasset trading process, these P2P exchange platforms may obtain fees from users, provide escrow services, and resolve user disputes, among other activities.

- *decentralised exchanges (DEXs)* - these are software platforms that rely on smart contracts to enable users of the platform to swap cryptoassets directly. For example, Binance, one of the world's largest bitcoin exchanges, recently launched a DEX that enables users to match trades directly and swap ERC20 tokens using smart contracts on the DEX platform but where no third party custody occurs.[16]

P2P exchange services of all varieties facilitate legitimate activity among cryptoasset users; however, our research and a number of prominent criminal cases indicate that some P2P exchange services are a common method of laundering funds in the cryptoasset ecosystem. In particular, individual P2P exchangers operating on dedicated platform sites present significant money laundering risks.

For example, in April 2019, FinCEN imposed penalties on an individual P2P exchanger who facilitated over $5 million in bitcoin trades as an unlicensed money transmitter, and who facilitated bitcoin exchanges on behalf of illicit online marketplaces by advertising trading services on P2P exchange platforms.[17] Similarly, in June 2018, a California woman was arrested for facilitating bitcoin trades with dark market vendors, after advertising her services on LocalBitcoins.[18]

It is unlikely that a single clear definition could be devised that captures the complexity of the business and service models that are described as P2P exchange services. Rather, the government could devise criteria that would enable it to assess whether a P2P exchange provider is more than just a passive website or platform enabling users to list their own trading services, but rather provides users with access to exchange services to which they would otherwise not have access, for example, either by collecting a fee from users or taking custody of user funds.

Any approach the government adopts should ultimately take into account the variety of P2P exchange models that exist and clearly articulate the circumstances under which they may be covered by regulation.

Other jurisdictions offer examples of this approach the government may wish to consider. In the US FinCEN has clarified that individual P2P exchangers have AML/CTF obligations. It has also clarified that P2P exchange platforms are exempt where they do

[16] See: https://www.binance.com/en/blog/32733469620032307 2/Binance-DEX-Launches-on-Binance-Chain-Invites-Community-Development

[17] See: https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money

[18] See: https://www.coindesk.com/localbitcoins-trader-bitcoin-maven-sentenced-to-year-in-prison

not receive funds and match user trades, but would have obligations to comply where they match user orders.[19] Finland in May 2019 adopted measures to implement 5AMLD that will apply to LocalBitcoins as an exchange business.[20]

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.

We feel that firms providing financial services related to the issuance of ICOs should be required to fulfil AML/CTF obligations. ICOs have been commonly associated with fraud, but Elliptic's research indicates that ICOs have in some instances been vehicles for money laundering activity.

In those scenarios, criminals (typically cybercriminals) identify a newly launched ICO. The criminals, acting under the guise of innocent token purchasers, send illicitly-obtained cryptoassets to the ICO issuers, who may be entirely unaware of their illicit origin, in exchange for the newly-minted coins. The criminal, now in receipt of 'clean' ICO tokens, can then exchange its ICO tokens for other untainted cryptoassets or for fiat currencies.

Much like the crypto-to-crypto exchange scenario, in this typology, the omission from AML/CTF requirements of the ICO issuer, or those facilitating sales of tokens on their behalf, results in a lack of oversight at a vital juncture in the money laundering process.

However, ICO issuers - or those facilitating sales of tokens on their behalf - are in a position to act as gatekeepers, identify token purchasers, conduct KYC on them, and apply other AML controls. At Elliptic, we have worked with ICO issuers who have sought information on the source of funds on cryptoassets used to purchase tokens, demonstrating the blockchain monitoring solutions can also be deployed to enable ICO issuers to scrutinise transactions.

We note as well that the FATF's revised definition of a virtual asset service provider covers those businesses engaged in the 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.' Addressing this category of service provider would therefore enable the UK to ensure its alignment with the FATF's requirements sooner rather than later.

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?

[19] See: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[20] See: https://localbitcoins.com/blog/aml-regulations-compliance/; https://news.bitcoin.com/finland-regulating-cryptocurrency/

Where applicable, how are firms conducting these due diligence checks, ongoing monitoring processes, and conducting suspicious activity reporting?

Though cryptoasset service providers have not been subject to AML/CTF requirements in the UK to date, we have observed many industry participants take proactive steps to apply AML requirements even in the absence of regulation. Many cryptoasset businesses located in the UK already utilise the cryptoasset-specific transaction monitoring software solutions we provide at Elliptic.

We have worked since 2014 with cryptoasset service providers operating in the UK to ensure that they have access to transaction monitoring solutions that allow them to detect suspicious activity among their customers and transactions, and to subsequently report that activity to law enforcement, even where they may not have an explicit requirement to do so under the UK's SAR reporting regime. We continue to receive frequent expressions of interest from new cryptoasset businesses that are establishing themselves in the UK and wish to have access to AML transaction monitoring solutions that will enable them to comply with the government's requirements once transposed.

Using Elliptic's blockchain monitoring solutions, our UK cryptoasset business customers are able to scrutinise their own customers' transactions and engage in risk-based activity monitoring. This includes scrutinising, for example:

- whether a customer's specific transactions may have been derived using funds from with a dark web marketplace or other illicit source;
- whether a customer's specific transactions may be destined for a cryptoasset address associated with a known illicit entity;
- the percentages of customers overall deposits or withdrawals that may have derived from or gone to illicit entities and actors.

To this end, we recommend that the government provide clarity for the private sector on the role that blockchain monitoring can provide in ensuring AML compliance, setting out its expectations for steps that regulated firms can take to ensure they have appropriate monitoring solutions in place to meet regulatory requirements. We discuss this further below in response to question 25 on privacy coins.

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?

As noted with regard to question 15 above, there is substantial evidence to suggest that money launderers and other illicit actors deliberately target jurisdictions where they know that AML/CTF regulation is absent or lax. Whilst the FATF's ongoing efforts to create a more robust and harmonised global regulatory framework for cryptoassets may reduce this regulatory arbitrage to a degree, we expect that criminals will continue to

seek out weak links in the global regulatory regime. This is likely to present substantial risks for the UK financial system even if it adopts other measures proposed in this report.

For example, if UK regulation applies only to cryptoasset businesses that are registered in the UK or have a physical presence here, cryptoasset businesses abroad that apply lower AML/CTF standards could potentially service UK customers without having to meet the UK's standards, creating an unlevel playing field and enabling criminals to move funds in and out of the UK with greater ease.

One potential solution for addressing this challenge would be to clarify that any AML/CTF requirements the UK adopts will apply not only to cryptoasset service providers with a physical presence in the UK, but to any that provide regulated services to individuals located in the UK.

This is the approach employed in the US that has allowed authorities to take action against cryptoasset businesses violating US AML/CTF requirements. FinCEN has clarified that money transmission requirements applicable to providers of cryptoasset services also extend to those businesses that provide substantial services to US persons, even where the service providers are located outside the US. In July 2017, FinCEN levelled a civil monetary penalty of $110 million against BTC-e, a now defunct exchange with operations across Eastern Europe that engaged in money laundering on a massive scale, but which serviced users in the US.[21]

We recommend the UK consider adopting a similar approach and extend its cryptoasset AML/CTF requirements to platforms and providers located abroad but servicing the UK market.

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?

We believe it is important that the government use the transposition of 5AMLD to address and clarify questions related to the management of risks surrounding privacy coins, but that it does so in a manner that does not stifle innovation or reasonable attempts of cryptoasset users to ensure privacy and confidentiality.

There is no single, accepted definition of privacy coins. Rather, privacy coins is an informal term that refers to a broad range of cryptoassets relying on technological innovations that enable varying degrees of transaction obfuscation, and that are generally impervious to the AML transaction monitoring solutions that are available for highly transparent coins, such as bitcoin and ethereum.

[21] See: https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

There are a number of legitimate uses for privacy coins. Individuals and businesses may reasonably wish to avoid having full details of their transactions recorded on public ledgers, as occurs with cryptoassets such as bitcoin. However, as noted above, we have observed the increasing use of privacy coins, particularly monero, in illicit finance.

For example, we have observed growing use of monero to pay for illicit goods and services on dark web marketplaces, including three of the largest five dark web marketplaces.[22] As described in response to question 17 above, we have also observed criminals using privacy coins as a layering tool in the money laundering process to obscure the flow of funds.

Exchanges or other service providers that offer their customers access to privacy coins can apply KYC/CDD measures to customers who use them. This can allow the exchange to determine if the customer presents any higher risk factors, and to mitigate associated risks. Where a customer purchases privacy coins in small amounts or infrequently, the associated risks may be lower.

However, at a transactional level, it is not possible to monitor customer activity in a manner that can be done for transparent coins such as bitcoin and ethereum, for which a complete audit trail of customers' activities can be obtained using blockchain analytics tools to ultimate source and destination of funds. Exchanges or other service providers will naturally have less visibility into their customers' transactional activity where privacy coins are used.

To mitigate these risks, the government should provide clarification about the factors cryptoasset businesses should consider when determining the appropriateness of AML/CTF controls they should apply based on the traceability features of a given cryptoasset.

This could include, for example, articulating expectations with regard to utilising blockchain monitoring solutions. Guidance could also articulate enhanced due diligence measures (EDD) that could be applied to satisfy regulators where a regulated business offers a privacy coin and where full transaction traceability is lacking.

A limited number of regulators globally have addressed how traceability can act as a factor in determining a risk based approach for cryptoasset product and service offerings. For example:

- The Hong Kong Securities and Futures Commission's regulatory sandbox framework for cryptoasset trading platforms requires that they 'employ technology solutions which enable the tracking of virtual assets through multiple

[22] See: https://uk.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUKKCN1SL0F0?il=0

transactions to more accurately identify the source and destination of these virtual assets.'[23] It also requires that platforms apply EDD for 'transactions involving virtual assets with a higher risk or greater anonymity (eg, virtual assets which mask users' identities or transaction details).'[24]

- The Abu Dhabi Global Market's (ADGM) Financial Services Regulatory Authority lists traceability as one factor it considers when assessing whether a cryptoasset offering is suitable, noting that before approving a cryptoasset businesses's listing of a token it considers whether 'transactions in the Crypto Asset can be adequately monitored.'[25] The ADGM's crypto asset guidance also notes that 'If a transaction is detected that originates from or is sent to a "tainted" wallet address belonging to a known user, that user should be reported . . . Currently, there are technology solutions developed in-house and available from third party service providers which enable the tracking of Crypto Assets through multiple transactions to more accurately identify the source and destination of these Crypto Assets. It is expected that [cryptoasset businesses] may need to consider the use of such solutions. . .'[26]
- FinCEN in May 2019 set out guidance that addresses privacy coins. FinCEN's guidance indicates that service providers may trade in privacy coins but must implement AML/CTF requirements in full where they do so. FinCEN's guidance also notes that many service providers 'comply with their [AML/CTF] obligations, in part, by incorporating procedures into their AML Programs that allow them to track and monitor the transaction history of a [cryptoasset] through publicly visible ledgers.'[27]

These approaches are notable because they do not attempt to ban or prohibit the use of privacy coins; rather, they acknowledge gradations in risk among types of cryptoassets based on their traceability features and provide indicators of risk-based measures and available solutions that firms can deploy to satisfy ongoing monitoring requirements.

Whatever approach the government adopts, we feel it is important that its regulatory framework clarify three key issues:

- Firstly, that there is a distinction in the nature of risk between different types of cryptoassets based on their relative traceability features, and that businesses should factor this into their risk based AML policies and procedures.

---

[23] See: https://www.sfc.hk/web/EN/files/ER/PDF/App%202_%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf, p7.
[24] Ibid, p. 6.
[25] See: http://adgm.complinet.com/net_file_store/new_rulebooks/g/u/Guidance_Regulation_of_Crypto_Asset_Activities_in_ADGM_140519.pdf, p. 12.
[26] Ibid, p. 26.
[27] See: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf, p21.

- Secondly, that blockchain monitoring solutions are available that can enable regulated firms in applying a risk-based approach to cryptoassets that have traceability features and that cryptoasset service providers should consider utilising these solutions where available.