GLOBAL
DIGITAL
FINANCE

June 10, 2019

VIA EMAIL:

Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

Her Majesty's Treasury (HMT)
Consultation on the Transposition of 5MLD
Sanctions and Illicit Finance Team (2/27)
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Re: Consultation regarding the Transposition of the Fifth Money Laundering Directive: April 2019

Dear HMT Team,

We support efforts by global standard setters, national authorities and regulators to consult and work with the nascent global digital/virtual asset industry.

To that end, we are hereby providing input to the Consultation regarding the Transposition of the Fifth Money Laundering Directive: April 2019.[1]

The input has been drafted and led by the GDF Advisory Council.

About GDF

Global Digital Finance ("GDF") is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets and digital finance technologies through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members—including some of the most influential digital asset and token companies, academics and professional services firms supporting the industry.

---

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf

GDF is proud to include Circle, ConsenSys, DLA Piper, Diginex, Hogan Lovells, Huobi and R3 as patron members.

The GDF Code of Conduct is an industry-led initiative driving the creation of global best practices and sound governance policies, informed by close conversations with regulators and developed through open, inclusive working groups of industry participants, legal, regulatory and compliance experts, financial services incumbents and academia. Code principles undergo multiple stages of community peer review and open public consultation prior to ratification.

For consistency, we have used the terms 'virtual assets' and 'virtual asset service providers' in our response, in line with the FATF Glossary.

Given the remit of GDF, we have concentrated our responses on the questions concerning virtual assets, and virtual asset service providers.

Consultation Inputs

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. 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 5MLD definition of virtual asset is focused on a digital representation of value that "is accepted by natural or legal persons as a means of exchange". It thereby appears focussed on payment/ exchange tokens. We believe this scope is appropriate.

We caution that a broader definition as suggested by the HMT to include tokens that represent "all relevant activity involving exchange, security and utility tokens tokens" possibly casts the net too broadly.

In particular, the GDF Taxonomy[2] distinguishes between Consumer Tokens, Payment Tokens and Financial Asset Tokens. Consumer Tokens (similar to so-called "utility tokens") should not be captured in AML regimes, especially when the tokens are being used for intended consumptive purposes - e.g. Ether paying for computation on the Ethereum blockchain, or a token being used like a movie ticket to attend a show, or a tokenised loyalty program such as airline miles.

These applications are currently not captured in AML regimes. Converting the tracking and awarding of such programs to a new technology, blockchain, should not trigger

[2] See https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Taxonomy-for-Cryptographic-Assets_Web-151018.pdf

them to be included in such regimes. Doing the opposite would constitute material overreach. It would also be very complex to enforce, even more so considering the number and variety of Consumer Tokens that may be developed in the future.[3]

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 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?

We refer to our answer to question 12 immediately above as regards to the proposal to include "all relevant activity involving exchange, security and utility tokens tokens" possibly casting the net too broadly.

As regards to wallets, there are many different types of wallets emerging, some of which are simply providing software-driven key management solutions for consumers, whilst others are providing a suite of functions and services that may make the wallet providers themselves into a custodian of digital assets.

These distinctions between wallet types and functions can impact regulatory status. For example, Australia has recognised that a digital wallet provider that simply provides a key management system and cryptographic key management is not necessarily providing a "designated service" meaning it is not necessarily regulated under the AML/CTF Act.[4]

We would agree with this position as it would be very challenging to enforce a broader definition. *As such, we suggest that non-custodial services, which can be defined as software that both generates keys and assists in key management but that at no time has access to user keys, be placed outside the remit of the UK's regime.*

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?

We have no objection to the FCA being assigned this role. We would, however, welcome the FCA creating tailored regimes where needed for virtual asset services and virtual asset service providers they would supervise, rather than to apply existent regimes without modification or consideration of the unique features and challenges of virtual assets and blockchain, some of which we have discussed in our earlier submissions to FATF and also in other work of the GDF.[5]

[3] See also P14-15 of our response to FATF on this important definitional point https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf
[4] See also P8-9 https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf
[5] See https://www.gdf.io/resources/

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?

In 2018 Europol highlighted that approximately EUR3-4 billion of criminal money is being laundered through cryptoassets linked to 1. their use to support black market transactions on the dark web, 2. theft through fraudulent ICOs, 3. hacks on echanges which as at the end of 2018 totalled $1.5billion, with $865m stolen from 6 hacks in 2018, and 4. sanctions evasions by state actors.

Given that it is estimated that between $800billion to $2trillion is being laundered through the global financial system annually, it is clear that the risks in the current virtual asset system are currently very small/less than 1% when compared to those in the traditional financial system.

In view of the above, it is sensible for the HMT response to be commensurate to those more limited risks at this time.

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?

The FATF has included virtual asset service providers offering "exchange between virtual assets and fiat currencies and between one or more virtual assets"[6] in its glossary with the updated guidance on the Interpretive Notes to Recommendation 15 that will cover virtual asset services providers due to be formally adopted by the FATF in June 2019.

Operators of cryptoasset ATMs fall within this definition[7] and in certain markets already require a money transmitter license given the connection to the fiat and debit card rails.[8]

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.

The FATF has included virtual asset service providers offering "exchange between virtual assets and fiat currencies and one or more virtual assets"[9] in its glossary with the updated guidance on the Interpretive Notes to Recommendation 15 that will cover virtual asset services providers due to be formally adopted by the FATF in June 2019.

[6] https://www.fatf-gafi.org/glossary/u-z/
[7] See also P11 for the results of a GDF survey https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf
[8] See https://coinatmradar.com/countries/ for BTC ATMs and https://coinatmradar.com/charts/top-operators/ for key operators. See also more detail on https://en.wikipedia.org/wiki/Bitcoin_ATM .
[9] https://www.fatf-gafi.org/glossary/u-z/

Similarly, a survey of the GDF community conducted in October 2018 viewed trading platforms as needing to be covered in the AML regime.[10] The GDF Principles for Token Trading Platforms also include principles on AML.[11]

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?

The survey of the GDF community conducted in October 2018 was more cautious on the practical feasibility of covering fully decentralised exchanges (DEX) in the AML regime.[12]

It is noted that blockchain technology enables a decentralised world where the exchange and settlement of digital tokens can occur on a direct "peer-to-peer" basis. Token holders can transfer tokens from their own personal wallet directly to another person's or entity's wallet.

This type of activity is often facilitated by smart contracts. People can build additional software platforms that, among other things, create graphical user interfaces utilising these smart contracts. These platforms are commonly referred to as "decentralised exchanges" or "DEXs". A DEX may operate autonomously, with no controlling entity that can be regulated or required to comply with AML/CTF requirements.

While there are many different interpretations of the term "DEX", currently the only reliable distinction between a centralised exchange ("CEX") and a DEX relates to custody - namely, a CEX maintains custody of its users' assets, while DEXs are "non-custodial" and do not obtain custody. As a result, unlike a CEX, a DEX may not maintain records about the identity of the parties to transactions, or may not conduct KYC/CDD.

Beyond that distinction, there is significant variation among so-called DEXs in terms of their function and operation, including with respect to whether they have order books and how they manage order matching and price negotiation.

In sum, it is important for the HMT to be specific about the definition and scope of the meaning of a DEX. We would recommend that where there is a central service provider (whether a natural or legal person(s)) that controls the users' cryptoassets or the keys thereto, or that derives income from or charges fees for its peer-to-peer matching or other services, it be treated the same as a CEX from a AML/CTF standpoint, i.e. it should be required to fulfil AML/CTF obligations on its customers where there is a UK nexus - that is, where the service carriers on business in the UK on onboards UK residents to its platform.

[10] See also P11 and P7-8 for a discussion of the distinction between CEX and DEX https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf

[11] https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Additional-Principles-For-Token-Trading_Web-151018.pdf

[12] See also P11 for the results of a GDF survey and P7-8 for a discussion of the distinction between CEX and DEX" https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf

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 survey of the GDF community conducted in October 2018 viewed smart contract developers, creators of open-source software and technology providers as needing to be outside the remit of the AML regime.[13]

Smart contract developers and technology providers should not be financial institutions (FIs) if they merely create a smart contract that is published and exists on a public blockchain.

Also, decentralised open-source protocols are not FIs. Protocols are software and by implication entirely and irrevocably deterministic. The rules are set in the code with no possibility to do anything other than what is laid out in the code.

Notwithstanding the foregoing, in order to mitigate possible AML/CTF risks associated with coding (e.g. a nefarious actor could create code that creates, embeds or heightens such risks), regulated FIs should exercise due care, skill and diligence when selecting, appointing and overseeing smart contract developers or technology providers, or when utilising existing smart contracts (e.g. open source code).

Where AML/CTF obligations do exist, it should be recognised that it may be reasonable in some circumstances to use the enhanced coordination/ communication capabilities of public blockchains to satisfy in whole or part the applicable KYC/CDD obligations.

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.

The FATF has included "participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset" in the remit of the definition of virtual asset service providers.

Similarly, the survey of the GDF community conducted in October 2018 viewed the issuance of ICOs as needing to be covered in the AML regime.[14] The GDF Principles for Token Sales and Token Sale Service Providers also include principles on AML.[15]

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?

As noted in our submission to FATF, cryptoasset service providers operating in jurisdictions that have made statements about future policy direction, or that have already issued guidelines or legislation bringing such providers in the remit of AML

[13] See also P4-5 https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf
[14] See also P11 and P7-8 for a discussion of the distinction between CEX and DEX https://www.gdf.io/wp-content/uploads/2018/10/GDF-Letter-to-FATF-dated-October-9-2018.pdf
[15] https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Additional-Principles-For-Token-Sales_Web-221018.pdf

regulation, are more likely to have started implementing normal course AML/CTF measures, including the below (R refers to FATF recommendations):[16]

1. Risk assessments (R1)
2. Sanctions screening for customers and payments and reporting of sanctions breaches (R6 and R7)
3. Customer Due Diligence (R10)
    a. KYC
    b. EDD
    c. Surveillance and transaction monitoring - both fiat/crypto and crypto/crypto
4. Record-Keeping (R11)
5. PEP name screening (R12)
6. Reliance on third parties, particularly with regards to CDD (R17)
7. AML staff training (R18) 8. SAR/STR reporting to local FIUs and law enforcement (R20)

We believe that a robust AML/ KYC approach should not require significantly greater overhead than a typical eMoney institution. However, the implementation of the FATF's proposed R16 (Wire Transfers) on cryptoasset services could have a devastating impact on efficiency, effectiveness, and overall compliance cost with little to no impact on the objectives that R16 seeks to achieve. The GDF responded extensively to this point in April 2019.[17]

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?

The GDF Community was established in order to develop Codes of Conduct that members can attest to. The GDF believes that the industry should act responsibly, and members are required to attest to the Codes. An AML/CTF Code of Conduct will be released for public consultation shortly in response to the GDF Community observation that there are virtual asset services providers operating with variable quality of AML programmes.

The GDF AML Working Group has been instrumental in the past few months in driving higher standards of AML governance across the global virtual asset service provider industry.

With regards to specific activities we see taking place within the GDF Community, we refer to our answer to question 21 immediately above.

[16] See also P18-19 https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf
[17] https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf

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?

There appears to be no definitive source of information with regard to this question. We have reviewed various sources and spoken within the GDF Community but do not believe at this time the answer is validated enough to present.

To improve data availability in the future, a new SIC code could for example be added to Companies House register. Existing VC firms can amend their current 4 digit code.

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?

Governments should be concerned about this. Unlike brick-and-mortar based business models, such as those common in traditional finance and which can be more easily supervised and enforced against within the jurisdiction(s) they are physically located in, technology services, including but not limited to cryptoasset services, can be offered from any location.

Lack of regulatory understanding, clarity and consistency as is currently prevalent in the case of cryptoassets, leads to various outcomes:

- Cryptoasset providers who want to comply with clear standards seek out jurisdictions where a license can be obtained and/ or where the regulatory regime has been adjusted to address the unique characteristics of cryptoassets, particularly jurisdictions that created new legislative regimes to attract such businesses and that are willing to take the risk to learn with them as they evolve;

- Cryptoasset providers that have no intention to apply higher standards of regulation unless and until regulatory consistency exists, will instead choose to operate from less regulated jurisdictions.

In other words, regulatory discrepancy creates room for regulatory arbitrage, sometimes justified - e.g. if a jurisdiction is ostensibly advanced on understanding a new trend and adjusting its regulatory regime for it - and sometimes unjustified - e.g. if the key motive is to locate in the weakest link jurisdiction in order to enable untoward activity.

It should also be noted that as was the case for many other novel technology related business models (e.g. Amazon, Uber, AirBnB, WeChatPay, Alipay, etc), different jurisdictions have different standing rulesets that may depending on the regulatory and political backdrop in that jurisdiction be easier or harder to reinterpret, change or adjust. Technology businesses being global or at least multi-jurisdictional (the latter is needed to scale), will typically choose to expand in markets where they feel they can make progress fastest, and will leave jurisdictions where they cannot.

This dynamic is heavily playing out in the cryptoasset sector at this time, especially given the rather extreme amount of regulatory discrepancy, including but certainly not limited to in the AML/ KYC space - e.g. many (including leading) jurisdictions have not yet applied standing AML ordinances, laws and regulations to cryptoassets, while others have. Platforms who locate in the former have a clear (by now muti-year) competitive

advantage over those in the latter. Regulatory discrepancy that continues for several years is a lifetime for technology related businesses.

In sum, it is critical for regulators to be more internationally coordinated, specifically on the policy setting level. It is equally critical that they be more internationally coordinated on the enforcement level by relying on existent investigation networks and MOUs.

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?

A customer's desire to protect their privacy is not necessarily in and of itself indicative of illicit activity. The desire to protect one's privacy, particularly the privacy of one's financial activity, is a legitimate one, as exemplified by the existence of legislation such as the GDPR. Additionally, growing awareness of the risks and dangers of privacy breaches (e.g. identity theft, the risk of manipulation of democratic processes) mean that some believe that privacy-preserving features will be necessary if digital currencies are to fulfil their potential, spurring interest in digital currencies that are implementing such features (including a desire on the part of some to purchase and hold such cryptoassets), and causing some existing cryptoassets (including Bitcoin[18] and Ethereum[19,20]) to lay plans to add privacy-preserving features. It's entirely possible that, in the future, some of the largest and most actively-used cryptoassets will evolve to become privacy coins.

While cryptoassets with privacy-preserving features have garnered a lot of attention for their perceived attractiveness for illicit activity, there is limited published evidence to suggest that the scale and extent of the risk they present is greater than other cryptoassets. If that were the case, it would be reasonable to expect that criminals would prefer to use such assets but that does not appear to be the case. For example, according to Chainalysis, "Bitcoin is by far the [criminals'] favourite. With our law enforcement customers, we see that over 95% of cases involve Bitcoin."[21]

If, in the future, there is a wholesale shift of illicit and criminal usage away from Bitcoin towards privacy coins, it may be necessary to re-evaluate the risk they posed but, at this point in time, any marginal risk due to the privacy-preserving features of such cryptoassets can be mitigated by ensuring that CDD measures are applied.

As a result, in many - and potentially the vast majority of - circumstances, particularly where the regulated entity has properly applied the appropriate CDD measures, the use of privacy coins will not be a high-risk factor. A technology-neutral risk-based approach, in which the regulated entity considers all the factors involved (e.g. whether the customer's transaction patterns match their stated purpose in trading cryptoassets, whether they can provide "off-chain" evidence to support their claimed source of funds, etc.) is appropriate.

[18] Pieter Wuille Unveils Two Proposals for Upcoming Bitcoin Privacy Soft Fork - Coindesk, 6 May 2019: https://www.coindesk.com/new-bips-hint-at-upcoming-taproot-bitcoin-soft-fork
[19] EIP 1922 - zkSNARK Verifier Standard: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1922.md
[20] Vitalik Proposes Mixer to Anonymize 'One-Off' Ethereum Transactions - Coindesk, 23 May 2019: https://www.coindesk.com/vitalik-proposes-mixer-to-anonymize-one-off-transactions-on-ethereum
[21] "Bitcoin Accounts for 95% of Cryptocurrency Crime, Says Analyst"- Fortune.com, 24 April 2019: http://fortune.com/2019/04/24/bitcoin-cryptocurrency-crime/

The fact that a regulated entity supports the trading of privacy coins or that a customer intends to trade a privacy coin has little impact on the regulated entity's ability to apply CDD measures[22]. In this respect, privacy coins are little different from other cryptoassets such as Bitcoin or Ethereum, and the same measures can be applied to, for example, identify the customer and any beneficial owners, assess the purpose and intended nature of the business relationship, obtain information regarding the customer's source of funds, and monitor the transactions between the customer and the regulated entity.

The sole difference, from a CDD perspective, between privacy coins and cryptoassets that lack privacy-preserving technologies, is that it may (depending on the cryptoasset in question) not be possible to trace the flow of funds through the asset's distributed ledger beyond the regulated entity's perimeter (i.e. either before they are received by or deposited with the regulated entity, or after they are withdrawn from or remitted by the regulated entity). Software tools that rely on the traceability of cryptoassets are commonly used by exchanges but they do not substitute for the rigorous application of CDD measures, and there are alternative methods for verifying customers' source of funds.

It is important to bear in mind that different "privacy coins" possess different qualities. For example, some provide support for "view keys:" that allow the person or entity that controls a payment address to grant a third party - such as a regulated entity, regulator or law enforcement investigator - the ability to view otherwise private transactions sent from that payment address, thus allowing the regulated entity to monitor transaction activity beyond their perimeter.

Depending on the circumstances involved (e.g. the extent to which the customer has a trading history with the regulated entity, the regulated entity's confidence in their understanding of the customer's source of funds) and the risk-based approach, it may be appropriate to conduct enhanced due diligence checks on the customer's source of funds and to file SARs/STRs as per normal process.

Therefore, assuming that regulated entities ensure that their CDD and AML processes take account of privacy coins and can trigger the use of enhanced due diligence measures and SAR/ STR filing when appropriate, the risks posed by privacy coins can be effectively managed alongside other cryptoassets, and no additional measures are necessary.

44. Is there a need for additional clarification in the regulations as to what constitutes "secure" electronic identification processes, or can additional details be set out in guidance?

It is the view of GDF that the government should utilise guidance to define the threshold and expectations for "secure" electronic identification methods. This would be would preferable to doing so through amendments to regulation.

As the government's consultation notes, the UK Money Laundering Regulations currently enables broad scope for firms to utilise a wide range electronic identification methods on a risk-sensitive basis. Attempting to define precisely what constitutes a "secure" method via changes to regulation could result in a definition that is too narrowly defined, creating

[22] For the avoidance of doubt, we are using the definition of "customer due diligence measures" that can be found in Article 13 of Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th AML Directive)

confusion or potentially dissuading firms from using certain electronic identification methods. Guidance offers a more dynamic format for addressing the standards and examples of electronic identification that may change over time and may need to be updated and amended as technological advancements and innovations occur.

45. Do you agree that standards on an electronic identification process set out in Treasury-approved guidance would constitute implicit recognition, approval or acceptance by a national competent authority?

We agree that inclusion of standards on electronic identification in Treasury-approved guidance, such as the Joint Money Laundering Steering Group (JMLSG) guidance would constitute implicit recognition of those standards by a national authority. The JMLSG guidance already includes detailed standards for firms to consider when undertaking electronic identification of customers and when conducting electronic identity checks and when selecting electronic data providers (see JMLSG 3.3.39 - 5.3.53). It would therefore provide the most appropriate and natural venue for addressing the standards of 5AMLD's secure electronic verification standards in detail.

46. Is this change likely to encourage firms to make more use of electronic means of identification? If so, is this likely to lead to savings for financial institutions when compared to traditional customer onboarding? Are there any additional measures government could introduce to further encourage the use of electronic means of identification?

GDF's membership includes virtual asset businesses with operations in the UK that already deploy electronic customer identification methods in the application of risk-based AML/CTF measures.

We therefore welcome steps the government may take to enable and promote the further use of electronic identification methods, and to clarify their appropriate use, as a robust electronic identification programme can provide a number of benefits to the financial sector including:

- Ability to use machine learning and advanced analytics to detect sophisticated impersonation fraud that can far surpass face-to-face onboarding;
- Creation of a frictionless online customer experience that can assist with the adoption of financial services products;
- Increased operational efficiency and effectiveness by automating previously manual tasks, thus lowering back office running costs with no compromise to compliance

As noted in response to the previous two questions, clear guidance, issued via JMLSG, on standards for secure electronic identification provides the most effective means for enabling firms to utilise electronic ID methods and techniques with confidence.

47. To what extent would removing 'reasonable measures' from regulation 28(3)(b) and (4)(c) be a substantial change? If so, would it create any risks or have significant unintended consequences?

For customers that are not listed nor regulated, further information is needed in order to mitigate the risk.

- Regulation 28(3)(b) requires additional information of customer identification (applicable law, board of directors name, the name of the person responsible for the operations…)
- Regulation 28(4)(c) requires further information on the ownership.

Both Regulations require two steps, (i) the identification and (ii) the verification of this identification. We recommend to treat differently the "identification" and the "verification".

Regulation 28(3)(b), as of today stipulates that "reasonable measures" must be taken for identification purpose and verification purpose, while Regulation 28(4)(c) requires "reasonable measures" must be taken only for verification purposes.

"*Reasonable measures*" implies an obligation of means and not an obligation of results. **We recommend to keep "reasonable measures" for the verification** part for both Regulations and **remove it for identification purposes**.

For Identification means, we suggest to replace "reasonable measures" with "is required to […]". This will imply an obligation of results to identify:

- Applicable laws, full name of board of directors, constitutional documents and the name of the person responsible for the operations;
- The beneficial owner ultimately controlling the customer.

For verification means, "reasonable measures" will imply that the obliged entity will have to demonstrate that it has taken the necessary amount of effort to verify the information and draw the appropriate consequences of a potential inability to verify.

Finally, we note the FATF definition of "Reasonable measure" in Recommendation 10(5)(b): "In determining the reasonableness of the identity verification measures, regard should be had to the ML/TF risks posed by the customer and the business relationship".

48. Do you have any views on extending CDD requirements to verify the identity of senior managing officials when the customer is a body corporate and the beneficial owner cannot be identified? What would be the impact of this additional requirement?

As per the FATF Recommendation 10, if no natural person is identified the relevant person is required to identify the natural person who holds the position of senior managing official.

The identification of senior managing officials in lieu of the beneficial owner must be the ultimate step to take. The inability to identify the natural person having ultimate

ownership must be properly documented to justify the need to identify the senior managing officials instead.

49. Do related ML/TF risks justify introducing an explicit CDD requirement for relevant persons to understand the ownership and control structure of customers? To what extent do you already gather this information as part of CDD obligations?

The ownership information is a crucial part of the CDD. Even where not clearly stipulated in the Regulation we understand that it is common practice for relevant persons to understand the ownership structure and identify the beneficial owner.

FATF Recommendation 10 refers to the beneficial owner as a "natural person" ultimately controlling the customer, whether directly or indirectly through legal person or arrangement

We recommend (i) to formalise this practice into the Regulation for avoidance of doubt and specifically, (ii) remind that beneficial owner refers to the ultimate **natural person** who owns and/or controls the customer.

50. Do respondents agree we should clarify that the requirements of regulation 31 extend to when the additional CDD measures in regulation 29 and the EDD measures in regulations 33-35 cannot be applied?

We agree that Regulation 31 should be extended to additional CDD measures. In addition to the measures outlined in Regulation 28, Regulation 29 describe additional CDD measures to be undertaken in specific situations.

51. How do respondents believe extending regulation 31 to include when EDD measures cannot be applied could be reflected in the regulations?

We propose a reasonableness test may be used in this situation, similar to the Proceeds of Crime Act s330(2)(b) "has reasonable grounds for knowing or suspecting" with regards to disclosure.

52. Do respondents agree the requirements of regulation 31 should not be extended to the EDD measures which already have their own 'inbuilt' follow up actions?

The GDF agrees that the requirements of Regulation 31 should not be extended in this circumstance.

53. Do respondents agree with the envisaged approach for obliged entities checking registers, as set out in this chapter (for companies) and chapter 9 (for trusts)?

We agree with HM Treasury's proposal that the requirement only apply to new business relationships. We further believe that this requirement should apply to business relationships established not only with companies and trusts that are required to register their beneficial owners in the UK, but also those that are required to do so in EU Member States, provided that the Member State in question has set up a beneficial ownership register.

54. Do you have any views on the government's interpretation of the scope of 'legal duty'?

We concur with the Government's interpretation on the scope of legal duty.

55. Do you have any comments regarding the envisaged approach on requiring ongoing CDD?

We agree with the proposed interpretation of the scope of 'legal duty' and the envisaged approach to ongoing CDD.

56. Are there any key issues that the government should consider when defining what constitutes a business relationship or transaction involving a high-risk third country?

In addition to a customer/ entity from a high-risk third country or transferring/ receiving assets to an account associated with a high risk third country, online financial services such as virtual asset exchanges and wallet providers should be diligent in identifying transactions initiated from IP addresses associated with high-risk countries, accounts with ultimate beneficial owners or key management personnel domiciled in high risk third countries and, for virtual asset services providers, wallet addresses that may not have direct transactions to high risk third countries but are linked to wallet addresses conducting transactions with high risk third countries.

57. Are there any other views that the government should consider when transposing these Enhanced Due Diligence measures to ensure that they are proportionate and effective in combatting money laundering and terrorist financing?

We propose expanding Enhanced Due Diligence requirements to not only transactions or business relationships involving a high risk third country, but also applying EDD to entities and individuals that may pose a higher risk based on a review of account activity. Within the virtual asset sector, higher risk activity where enhanced due diligence may be needed can include frequent transactions to addresses that have been linked to extortion, ransomware, sanctions or other illicit activity, accounts involved with multiple SAR filings and accounts conducting large transfers which frequently change profile information and beneficial owners.

59. Do you agree that the UK functions identified in the FCA's existing guidance on PEPs, and restated above, are the UK functions that should be treated as prominent public functions?

We agree with the UK functions identified by the FCA's existing guidance on PEPs. We believe that UK functions should be treated as prominent public functions and thus would trigger additional EDD requirements such as (i) senior management approval, (ii) determine source of wealth and funds involved, and (iii) conduct Enhanced Due Diligence.

In addition to the definition mentioned above, for state owned enterprises, key managers such as the C-suite could also be included. Even if not mentioned in the above definition, family members and close associates of a PEP should also identified and EDD triggered, where appropriate.

60. Do you agree with the government's envisaged approach to requesting UK-headquartered intergovernmental organisations to issue and keep up to date a list of prominent public functions within their organisation?

The approach of requesting UK-headquartered intergovernmental organisations to issue and keep up to date a list of prominent public functions within their organisation may seem to ease the identification of PEPs within this type of organisations. However, we may have doubts on the following two points: (i) who would be responsible for taking the decision that the position is considered as meeting the requirements and (ii) who would be responsible to ensure that the list is exhaustive and kept up to date.

61. Do you have any views on the proposal to require obliged entities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?

Please see our response to question 63.

62. Do you have any views on the proposal to require competent authorities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?

Please see our response to question 63.

63. How should discrepancies in beneficial ownership information be handled and resolved, and would a public warning on the register be appropriate? Could this create tipping off issues?

We believe that the accuracy and reliability of the information held on the Companies House public register is key to preventing the well-documented abuse of UK legal entities for money-laundering purposes. We therefore support the proposal with caveats to require obliged entities and competent authorities to inform Companies House of the discrepancies they identify.

Our caveat to support is that obliged entities and competent authorities already have significant obligations, and this requirement may reduce the effectiveness and efficiency of compliance operations whilst increasing costs. It may also lead to duplication say, where two obliged entities report the same discrepancy at the same time.

Therefore, in order to ensure that this additional burden on obliged entities is proportionate to its benefits for the prevention of money laundering, it is necessary for Companies House to have the capacity to effectively resolve reported discrepancies, and to consider performing an initial due diligence when companies are formed and on periodic refresh. A concern we also highlight is how Companies House would seek to correct any discrepancy, and whether this information will be validated or whether Companies House will rely again on obliged entities and competent authorities to act on its behalf in providing the validation.

HM Treasury further asks how discrepancies should be resolved, and whether a public warning on the register would be appropriate, as well as whether such a warning could create tipping-off issues.

Given that the notification of a discrepancy does not necessarily entail the submission of a Suspicious Activity Report, it does not appear that tipping-off concerns arise under the Proceeds of Crime Act 2002. However, a public warning on the Companies House register would alert the person concerned that a notification has been made and, depending on the circumstances, potentially enable them to identify the obliged entity that has reported the discrepancy. In this regard, it may be necessary for Companies House not to flag a discrepancy until first attempting to obtain updated evidence.

75. Do you have any views on the best way for trustees to share the information with obliged entities? If you consider there are alternative options, please state what these are and the reasoning behind it.

Another alternative option would be to allow the trustee to determine a list of obliged entities that could access the TRS database. This would not only ease the onboarding but also the review cycle of the trust and ease the identification of change of key information of the trust.

76. Do you have any comments on the proposed definition of legitimate interest? Are there any further tests that should be applied to determine whether information can be shared?

We believe that the proposed definition legitimate interest might be a good first step to determine if access can be granted to the information to only the people that would need to access it in order to fight against money laundering and terrorist financing. We believe the second and third criteria might be difficult to implement and ensure compliance with GDPR standards.

Another option to strengthen the second and third criteria might be for the requester to (i) provide its assessment that led to the request to the TRS and (ii) explain how the data will be used once accessed.

77. Do the definitions of 'ownership or control' and 'corporate and other legal entity' cover all circumstances in which a trust can indirectly own assets through some kind of entity? If not, please set out the additional circumstances which you believe should be included, with rationale and evidence.

Based on the above definitions, most circumstances in which a trust can indirectly own assets through some kind of entity should be covered. The "Ownership or control" definition should be necessary and broader enough to identify the interest a trust may have in any corporate or other legal entity. The 25% threshold could be reduced to 10% when dealing with a trust deemed to represent higher risk of money laundering or financing terrorism.

78. Do you have any views on possible definitions of 'other legal entity'? Should this be defined in legislation?

The "Corporate and other legal entity" definition could include partnerships as well as family offices. Definition in the legislation would reduce the interpretation of this form of entity and would ensure consistency in its application.

79. Does the proposed use of the PSC test for 'corporate and other legal entity', which are designed for corporate entities, present any difficulties when applied to non-corporate entities?

It may be that a specific definition is required for non-corporate entities that better encompasses the entity type. For example, in the case of a trust and in certain circumstances, it is not a shareholding that determines control as opposed to a trustee or board of trustees who would not have a percentage holding. This may be best placed into guidance rather than legislation

80. Do you see any risks or opportunities in the proposal that each trust makes a self-declaration of its status? If you prefer an alternative way of identifying such trusts, please say what this is and why.

The limitation of self declaration will be that obliged entities will not have any way to verify the declaration.

An alternative option could be to provide tax return of the trust that should list the ownership and controls interest of the trust as a basis to calculate its taxes.

81. The government is interested in your views on the proposal for sharing data. If you think there is a best way to share data, please state what this is and how it would work in practice.

Where data is required to be shared with obliged entity it may be possible to utilise Government Gateway services for authentication of appropriate obliged entities and then provide either a user interface (portal) or machine interface (Application Programmers Interface, or API) into the data.

It should not be possible to take a full download of the data (as is the case for Companies House data) but rather only access data on the basis of known factors (for example, being provided with a unique ID by the obliged entity's client). In this way, the data can be maintained securely without releasing data in an uncontrolled fashion.

Access will also need to be proactively managed such that if an obliged entity is no longer licensed, access is immediately revoked.

An alternative option would be a push mechanism whereby the obliged entity's client can push a request from the register to the chosen obliged entity, although this mechanism will be more difficult to manage where data needs to be sent to a team or direct to a system as opposed to an individual within the obliged entity.

104. Should regulation 19(4)(c) be amended to explicitly require financial institutions to undertake risk assessments prior to the launch or use of new products, new business practices and delivery mechanisms? Would this change impose any additional burdens?

We draw attention here to the European Supervisory Authorities' paper of January 2018 'Opinion on the use of Innovative Solutions by Credit and Financial Institutions in the CDD Process' [23], and in particular the article 17(a):

> *"Before introducing an innovative solution in their CDD process, the ESAs believe that firms should carry out a full assessment of the solution to ensure that it has undergone proper testing and to establish whether or not the solution allows the application of CDD measures in line with firms' AML/CTF policies and procedures and applicable AML/CTF law. "*

Therefore, we believe that it should be explicitly required that such an assessment is made prior to the use of new technologies.

We hope you may find our response helpful. Please do not hesitate to contact our Executive Director, Teana Baker-Taylor (Teana@gdf.io) or either of our AML working group co-leads, Benedicte Nolens (benedicte@gdf.io) or Malcolm Wright (malcolm.wright@diginex.com) for further questions or comment.

[23] https://eba.europa.eu/-/esas-publish-opinion-on-the-use-of-innovative-solutions-in-the-customer-due-diligence-process