DIGITAL CURRENCIES
Governance Group

Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022

OCTOBER 14, 2021

Digital Currencies Governance Group (DCGG) is an international industry body with the aim to provide regulators with unbiased information, best practice knowledge and expert industry-related insights on policies concerning crypto-assets.

DCGG represents the full spectrum of key stakeholders in the ecosystem, including Tether – the biggest stablecoin issuer worldwide, Hermez – pioneer Layer 2 technology for scaling payments, Bitfinex – top tier digital assets exchange, Iden3 – avant-garde player in blockchain-based identity management, and others.

DCGG creates an open dialogue and encourages the communication between political representatives and digital currencies experts to ensure that legislation supports scale and innovation in the crypto-asset space.

GENERAL CONSIDERATIONS

DCGG welcomes the consultation to amend the Money Laundering Regulations (MLRs). Our members represent some of the largest cryptoasset businesses globally and we operate cross-border. For us, having **a clear, proportionate and internationally harmonised AML regulation is key**. Harmonisation with the international rules is also a considerable factor for many businesses, including in the cryptoasset industry, when it comes to the choice of relocating their operations and directly contributing to the country's economy. DCGG and its members welcome the ability to protect our customers without regulatory ambiguity or divergences at the cross-border level, thus it is of high importance to ensure that the UK regulations would be harmonised with the international rules

Information gathering

Question 52. In your view, is it proportionate for the FCA to have similar powers across all the firms it supervises under the MLRs? Please explain your reasons.

Regulation 74A grants the FCA very broad powers and they can require cryptoasset businesses to provide information as directed by the FCA and at a frequency or form that the FCA specifies. This regulatory ambiguity and uncertainty can lead to significant burdens for the cryptoasset industry and are not in all cases proportionate to the risks present in the cryptoasset industry.

It is important that cryptoasset businesses, especially those that provide cross-border services, can benefit from regulatory and supervisory certainty, as well as a level-playing field. The FCA's powers should be similar across all the firms it supervises and should not put the cryptoasset businesses at a disadvantage. It is important to ensure that any cryptoasset business is not by definition considered more risky, and thus automatically subject to more ad-hoc and broader information gathering and supervisory powers due to their nature (centralized or decentralized) but that there is a consistent approach across the financial services industry.

TRANSFERS OF CRYPTOASSETS

Question 56. Do you agree with the overarching approach of tailoring the provisions of the FTR to the cryptoasset sector?

DCGG agrees that it would not be feasible to simply expand the scope of the FTR to include cryptoasset firms, but due care must be taken to adapt the provisions of the FTR to reflect the particularities of the crypto sector, notably with regards to how transfers of cryptoassets are made and the current lack of standardised technology solutions for full compliance.

Question 58. Do you agree that a grace period to allow for the implementation of technological solutions is necessary and, if so, how long should it be for?

DCGG welcomes the UK government's earlier decision to defer the implementation of FATF's "travel rule" to allow for compliance solutions to be developed. However, we believe that it is too premature to implement the travel rule currently and the grace period should be extended.

The data accompanying crypto-asset transfers still varies widely in quality and standards. The messaging and reporting data standards in the crypto asset industry are not yet set, although industry initiatives have aspired to address this gap. To this end, the ability of a cryptoasset service provider to seamlessly integrate information accompanying transfers coming from multiple other service providers will be hindered. This lack of standardization raises the cost of compliance and increases time needed to comply as well.

Similarly, cryptoasset businesses have not yet been able to solve the "discovery" problem associated with the travel rule from a technical point of view. More concretely, when there is an exchange of funds between two compliant cryptoasset businesses that both have implemented the travel rule, there is no issue. However, in cases where a compliant cryptoasset business received funds from a non-compliant cryptoasset service providers, it is difficult, and at times impossible, for the compliant cryptoasset business to differentiate whether the sender of the funds is a private self-hosted wallet or a non-compliant cryptoasset business.

Consequently, we would suggest extending the grace period by 24 months to allow for further international standardization to emerge and make it possible for cryptoasset businesses to comply with the rule.

Use of provisions from the Funds Transfer Regulation

Question 59. Do you agree that the above requirements, which replicate the relevant provisions of the FTR, are appropriate for the cryptoasset sector?

DCGG understands that, as in the FTR, the information that must accompany the transfer will depend on its value and whether all cryptoasset service providers involved in the transfer are carrying on business in the UK. We would urge for clarity on the latter point, given the global nature of our industry. Does a "domestic transfer" constitute a transfer between two users, resident in the UK, or between two CASPs licensed in the UK, irrespective of where the users are? In DCGG's view, the former interpretation achieves the objectives of this requirement.

Furthermore, DCGG understands that where the required beneficiary or originator information is missing, the cryptoasset service provider receiving the transfer must decide, on a risk-sensitive basis, whether to ask for the required information before or after making the cryptoasset available to the beneficiary. Our view is that such risk-weightings should be determined at an industry level, possible subject to shared Codes of Conduct.

DCGG appreciates that the receiving cryptoasset service provider will be required to retain the beneficiary and originator information for a period of five years from the date it reasonably believes the transaction is complete. However, given the immutable nature of the DLT ledger, the requirement to delete data can only apply to non-DLT systems. This is, in turn, mandating that the industry uses non-DLT systems to comply with the Travel Rule, which may not be a forward-looking requirement, as it not a technology neutral requirement.

Similarly, while we are keen to reconcile GDPR requirements with the realities of the distributed ledger technology, there are a number of areas where the two do not work easily together. We would ask HMT and the national competent authorities to issue guidelines on this issue before requiring any compliance.

DCGG understands that Cryptoasset service providers will be required to make information available fully and without delay in response to a written request by the FCA, HMRC, the NCA or the police, where this information is reasonably required in connection with the Authority's functions:

- We encourage the Government to ensure the legislative framework leaves the possibility of competent authorities and enforcement agencies to participate in DLT networks in order to have real-time visibility of the information shared in them.
- In a similar vein, Travel Rule compliance products can be co-developed with the public sector to ensure similar level of transparency – be they on DLTs or not.
- Finally, the requirement to share data quickly should not become a barrier to adopt innovative solutions, like Zero Knowledge Proof, which have, so far, shown superior results in addressing privacy concerns.

Provisions specific to cryptoasset firms

Question 60. Do you agree that GBP 1,000 is the appropriate amount and denomination of the de minimis threshold?

DCGG understands that this threshold is consistent with the de minimis exemption available to wire transfers, yet we encourage HMT to consider the impact of such a limit in relation to the function that crypto-assets perform in society. Often, when crypto-assets are used as a remittance vehicle, it is because they offer a more cost-effective alternative to fiat transfers. Towards this financial inclusion role, a higher exemption will not burden higher-value transfers with the cost of compliance, meaning that more lower income workers can send money home more efficiently.

Furthermore, we strongly encourage HMT to set clear parameters on when the GBP 1,000 value should be calculated in a transfer cycle. We suggest it is most fair to users that this calculation is made at the point in time when a user orders the transfer. Finally, we firmly agree that the exchange rate between the crypto-asset being transferred and GBP should be determined by each individual VASP. Much like any other exchange bureau, setting these rates is subject to industry competition.

Question 61. Do you agree that transfers from the same originator to the same beneficiary that appear to be linked, including where comprised of both cryptoasset and fiat currency transfers, made from the same cryptoasset service provider should be included in the GBP 1,000 threshold?

While DCGG supports the Government's objective to ensure that the de minimis threshold is not abused, we urge for a review of the notion of 'being linked' in the context of crypto-asset markets. For instance, if an investor trades actively in small sums during the course of a day, a reasonable solution is to treat each transfer as separate. The aim of such activity is to execute a trading strategy, and neither each individual transfer, nor all transfers combined, would seek to add money laundering risk to the system. Importantly, technologies exist to spot such patterns and determine their most likely risk profile – this is equally true for transfers in crypto-assets and for transfers in fiat. Such risk-based approach should be permissible when determining whether transactions are linked (fiat transactions included) or not.

Question 62. Do you agree that where a beneficiary's VASP receives a transfer from an un-hosted wallet, it should obtain the required originator information, which it need not verify, from its own customer?

DCGG firmly supports initiatives which discourage any non-transparent or illicit use and abuse of crypto-assets.

To this end, we do suggest that if transfers originating from an un-hosted wallet are made to a wallet hosted on one of our Members' platforms, such transfer should fall out of scope of reporting requirements.

If this is unavoidable, then the liability of the beneficiary should be limited to obtaining but not verifying the information of the sender. We note that in this scenario, the owner of the un-hosted wallet need not necessarily have been a customer of the VASP.

Question 63. Are there any other requirements, or areas where the requirements should differ from those in the FTR, that you believe would be helpful to the implementation of the travel rule?

DCGG would point HMT's attention to the crypto-asset community's contribution to developing industry-led standards for compliance with the Travel Rule, particularly among centralized crypto-asset exchanges. This is vital, as it is the crypto-asset industry's "SWIFT" moment. We are deploying the innovative and collaborative spirit of our community to establish an efficient global messaging standard, which is appropriate for DLT Technology. We do believe that HMT should seek to monitor this process and align the enforcement of transparency requirements on crypto-transfers with the emergence of such standards. Both traditional payments and the UK's approach to Open Banking provide sound evidence of the value of such public-private approaches to regulation can bring for end customers.

What is more, *DCGG suggests that a helpful course of action in relation to the Travel Rule would be to leverage the UK's excellence in Regulatory Sandbox, pioneered by the FCA*. This is commonly enacted within the crypto-asset industry and allows for a period of time where industry actors are allowed room to become aligned and compliant with novel regulation. Sandbox testing is recommended and currently implemented by the FCA; therefore, this approach is befitting to the current crypto-asset marketplace in the UK. DCGG recommends a sandbox that allows crypto-asset exchange providers to slowly role out FTR solutions on a risk-based approach and continuously expand the scope of Travel Rule-compliant transfers. That way, the industry can meaningfully collaborate, under the supervisor's watch, on shared and accepted standards. It is important, of course, that the legislator is prepared to learn from a Sandbox trial and adapt the legal framework accordingly.