

August 4, 2022

Further EU and UK Developments in Financial Crime Regulation of Cryptoassets

While cryptocurrency markets have been experiencing significant fluctuation in value and stability, regulators have continued progressing proposals to further regulate virtual assets and virtual asset service providers (“VASPs”). This Alert provides a brief overview of some of the developments in anti-money laundering/counter-terrorist financing (“AML/CTF”) and sanctions regulations, focusing on brief updates from the Financial Action Task Force (“FATF”), the European Union and United Kingdom, as well as the United States.

Attorneys
[Melissa C. Bender](#)
[Eve Ellis](#)
[Helen Gugel](#)
[Paige Berges](#)
[Dorota Maj](#)
[Brad A. Rocheville](#)

I. Financial Action Task Force

In June, FATF released a *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*.¹ This report sought to evaluate countries’ implementation of the recommendations in FATF’s initial *2019 Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (updated in October 2021 – see our previous Alert [here](#)) – in particular focusing on the “Travel Rule”² and Recommendation 15 (requiring that VASPs be regulated for AML/CTF purposes). According to the report, the “vast majority” of jurisdictions have not fully regulated VASPs in line with Recommendation 15 and/or require major or moderate improvements in implementation.³ Similarly, FATF found that most jurisdictions have made only “limited progress” in introducing the travel rule for VASPs – in part because many jurisdictions are “still deciding on which approach to take” on issues such as unhosted wallets, *de minimus* thresholds, and data privacy issues. On a positive note, FATF notes that the private sector has made progress facilitating the implementation of the travel rule, both providing technical solutions and proactively seeking to voluntarily comply.

FATF concludes that it will continue to monitor countries’ progress implementing the FATF recommendations, and work with countries to consider appropriate measures to apply to unhosted wallets, decentralized finance (“DeFi”) and non-fungible tokens (“NFTs”), which the FATF report identifies as particular risks and areas for focus over the next year.

II. European Union

In June 2020, the Council presidency and European Parliament reached a provisional agreement related to the transparency of cryptoasset transfers in the *Markets in Crypto Assets (“MiCA”) proposal*.⁴ The proposal covers a broad range of regulations related to stability and consumer protection and overall providing legal certainty and uniform rules related to virtual assets and VASPs. The proposal also includes AML/CTF requirements, including a proposal to apply the FATF “travel rule” to VASPs (termed “crypto asset service providers”) regardless of amount, in part to mitigate “smurfing” – which occurs where a money launderer breaks money up into smaller transactions to avoid scrutiny.

The proposal also provides that verification of transaction data between hosted wallets (by a VASP) and unhosted wallets should only be required in the following circumstances: they are over EUR 1,000, the unhosted wallet is controlled by the VASP’s client, and on a risk-basis. The same conditions will apply to transfers between EU VASPs and non-EU VASPs. However, transfers between unhosted wallets will remain out of scope. Additionally, under the new proposed regulations, VASPs must implement suitable internal policies, procedures, and controls to comply with AML/CTF requirements. Furthermore, EU member states will be required to demonstrate that crypto asset service providers are obliged entities pursuant to the 4th AML directive.⁵ These new regulations are expected to come into force in 2023/2024. The proposal also confirms that sanctions already apply to persons operating in the crypto currencies sector.

Recent EU sanctions related to Russia include a prohibition on providing crypto asset wallet, account or custody services (if the wallet value exceeds EUR 10,000) to Russian nationals or natural persons residing in Russia or legal persons, entities or bodies established in Russia.⁶ The European Union has also released FAQs clarifying that all transactions

prohibited by EU sanctions “are also prohibited if carried out in crypto-assets” the same as they would be in fiat currency. The EU also warns that cryptoassets should not be used to “circumvent” sanctions restrictions.

III. United Kingdom

In June 2022, HM Treasury published the outcome of and proposed response to its 2021 consultation on the proposed amendments to the UK *Money Laundering Regulations 2017* (“MLRs”).⁷ Following approval by Parliament, the amendments will come into force on 1 September 2022. There are a number of proposals related to VASPs. The UK will maintain information-sharing (travel rule) requirements for VASPs (termed cryptoasset businesses) including intermediaries, despite some respondents feedback that the information required was disproportionate to illicit finance risk. The amended regulations will make clear however that, where an intermediary is involved, the travel rule applies only to cryptoasset exchange providers or custodian wallet providers and not all intermediaries such as software providers. The proposals include an exemption for transfers involving only UK-based VASPs – however the information must be made available on request (noting that this should be shared via a different, private system and not “on chain”).

The UK proposes to modify the thresholds to apply the travel rule to cryptoasset transfers of EUR 1000 or more (as this is less than GBP 1,000 at current exchange rates) and in line with FATF recommendations. In calculating this threshold, cryptoasset transfers should be treated separately to fiat transfers in determining whether the *de minimis* threshold is cumulatively reached. The UK proposes to allow a 12-month grace period (up to September 2023) for firms to implement the travel rule.

The UK proposes to require collecting information from both parties of unhosted wallet transfers only to transactions which pose an “elevated risk of illicit finance”. The final legislation will set out minimum factors that firms must consider in determining “elevated risk”. The UK concludes that it “does not agree that unhosted wallet transactions should automatically be viewed as higher risk”. The report notes that there are valid reasons for using an unhosted wallet, including customizability, but is “conscious” that leaving unhosted wallets completely unregulated may incentivize criminals to use them to evade controls. The government will not propose verification requirements however for information collected on unhosted wallet transfers.

Furthermore, the proposed regulations provide that the government will no longer require that a *de minimis threshold* apply to both fiat currency and crypto-asset transfers. Instead, crypto-asset transfers will be treated separately. Further, the UK threshold has been lowered to EUR 1,000 before the “travel rule” applies. While this may be viewed as the government taking a lenient approach to AML/CTF, it corresponds with the thresholds set by the EU and FATF. As such, this decision will align regulations across borders and standardize processes. In response to concerns that changes to the “travel rule” may require the implementation of technological solutions, the government explained that they will allow a 12-month grace period for companies to adapt their internal procedures.

The Law Commission has also [published](#) new proposals to reform digital asset-related laws. Although it does not cover AML/sanctions proposals, it does note that the “majority of users” use privacy-enhancing mechanisms for personal privacy-related reasons, rather than for conducting illicit transactions.

With respect to sanctions, the United Kingdom has issued several updates to ensure UK persons are aware that cryptoassets are considered “funds” and “economic resources” for the purpose of economic sanctions restrictions,⁸ and UK persons – in particular regulated entities – are expected to evaluate red flag indicators of sanctions evasion including in the use of cryptoassets.⁹ Regulated entities have a duty to inform the UK sanctions regulator, the Office of Foreign Sanctions Implementation (“OFSI”) of suspected sanctions breaches; from August 30, 2022 this obligation will be expanded to crypto-asset exchange providers and custodian wallet providers that are registered with the Financial Conduct Authority.¹⁰

IV. United States

In March 2022, the United States issued an executive order on *Ensuring Responsible Development of Digital Assets*¹¹ outlining objectives to ensure that regulations are put in place to safeguard consumers, investors, business and the financial system - including to ensure that players are subject to appropriate regulatory and supervisory standards. In particular, the EO states “[i]llicit actors, including the perpetrators of ransomware incidents and other cybercrime, often launder and cash out of their illicit proceeds using digital asset service providers in jurisdictions that have not yet effectively implemented the international standards set by the inter-governmental Financial Action Task Force (FATF).” Accordingly, a key priority for the United States is to “mitigate the illicit finance and national security risks posed by misuse of digital assets.”

In June, a bill was introduced related to regulating virtual assets, which would require provisions to be set out related to anti-money laundering and sanctions compliance responsibilities of certain players in the virtual asset space, although it does not attempt to do so within the text of the bill itself. See also our previous Alert [here](#).

Further, on June 6, 2022, in response to the directive from President Biden mentioned above, the U.S. Department of Justice (“DOJ”) published a report on how to strengthen international law enforcement cooperation for detecting, investigating and prosecuting criminal activity related to digital assets.¹² The report was spearheaded by the agency’s nascent National Cryptocurrency Enforcement Team (“NCET”), which is led by former Southern District of New York prosecutor Eun Young Choi. Incidentally, Ms. Choi’s appointment in February 2022 coincided with the Federal Bureau of Investigation’s (“FBI”) announcement the same month creating a Virtual Asset Exploitation Unit and an International Virtual Currency Initiative.

In addition to federal efforts, individual states are taking action to target anti-money laundering violations. Recently, the New York Department of Financial Services fined a popular cryptocurrency exchange \$30 million after the agency found that the firm had inadequate anti-money laundering and cybersecurity compliance controls.¹³ In particular, the firm inadequately monitored transactions, insufficiently staffed its anti-money laundering unit, and failed to comply with state cybersecurity guidelines.¹⁴ As a result, the company is required to engage an independent compliance consultant to monitor the firm going forward.¹⁵

V. Conclusion

As expected, this year has seen significant activity from governments and regulatory bodies seeking to monitor VAs and VASPs, and ensure adequate implementation of AML/CTF and sanctions standards. Stakeholders in the cryptoasset industry should evaluate where regulations are anticipated and proactively put in place compliance controls to lessen the likelihood of involvement in money laundering or sanctions breaches.

For firms dealing with or looking to enter into the virtual currency space, please contact the Ropes & Gray team.

1. Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (2022), <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>.
2. The “travel rule” applies to wire transfers taking place between two obliged entities. FATF recommends this applies where the transaction is USD/EUR 1,000 or more. The obliged entities must ensure certain information “travels” with the transaction to the recipient entity to allow for screening and monitoring.
3. FATF found only 29 of 98 countries require VASPs to implement the travel rule, and only eleven countries the FATF surveyed are actively enforcing and supervising compliance. (Note FATF does not disclose which countries in its report).
4. Council of the European Union Press Release, *Anti-Money Laundering: Provisional Agreement Reached on Transparency of Crypto Asset Transfers* (June 29, 2022), <https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/>.
5. *See* Directive (EU) 2015/849 (4th Anti-Money Laundering Directive, 4AMLD) of May 20, 2015, *Prevention of the use of the Financial System for the Purposes of Money Laundering or Terrorist Financing*.
6. *See* Council Regulation (EU) 833/2014 art. 5b(2) of July 31, 2014, *Concerning Restrictive Measures in View of Russia’s Actions Destabilising the Situation in Ukraine, 2014 O.J. (L 229)*.
7. *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2022 (Eng.)* <https://www.gov.uk/government/consultations/amendments-to-the-money-laundering-terrorist-financing-and-transfer-of-funds-information-on-the-payer-regulations-2017-statutory-instrument-2022>
8. Office of Financial Sanctions Implementation, *UK Financial Sanctions: General Guidance for Financial Sanctions Under the Sanctions & Anti-Money Laundering Act 2018* (July 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1094659/General_Guidance_-_UK_Financial_Sanctions_Jul_2022_.pdf.
9. *See* Financial Conduct Authority, *Joint Statement from UK Financial Regulatory Authorities on Sanctions and the Cryptoasset Sector* (Mar. 11, 2022), <https://www.fca.org.uk/news/statements/uk-financial-regulatory-authorities-sanctions-cryptoasset-sector>.
10. *See* the UK Sanctions (EU Exit) (Misc. Amendments) Regulations 2022 and the Sanctions (EU Exit) Miscellaneous Amendments) (No. 2) SI 2022/818 (July 2022).
11. Exec. Order No. 14,067, 87 Fed. Reg. 14,143 (Mar. 9, 2022), <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-ensuring-responsible-development-of-digital-assets/>.
12. *See* The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14,607: *How to Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets* (Jun. 6, 2022), <https://www.justice.gov/ag/page/file/1510931/download>.
13. *See* Derek Saul, *Robinhood’s Crypto arm hit with \$30 Million Fine by State Regulator*, *Forbes* (Aug. 2, 2022), <https://www.forbes.com/sites/dereksaul/2022/08/02/robinhoods-crypto-arm-hit-with-30-million-fine-by-state-regulator/amp/>.
14. *Id.*
15. *Id.*