WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

EU Extends "Travel Rule" to Crypto Asset Service Providers, Raising Data Privacy Concerns

August 12, 2022

AUTHORS

Laura E. Jehl | Britt Mosman | Nikki M. Cronin | Kari Prochaska
Amal Ibraymi

Recently, several notable legal and regulatory developments have impacted the European digital assets and financial technology sector. On June 29, 2022, the European Parliament and Council reached an agreement to update the rules on information accompanying the transfers of funds to extend the scope of those rules to include transfers of crypto assets.[1] The proposed rule is anticipated to come into effect in July 2024.

Crypto assets are digital assets built on a distributed ledger technology, such as a blockchain, and rely on cryptography and peer-to-peer networks to create, verify, and secure transactions (e.g., Bitcoin, Ethereum). Under the proposed rule, known as the "Travel Rule," the scope of Regulation 2015/847 on information accompanying transfers of funds would be extended to include transfers of crypto assets made by Crypto Asset Service Providers ("CASPs"). Further, extending the compliance requirements of the EU Travel Rule is intended to make it more difficult for cybercriminals to misuse crypto assets for criminal purposes, such as money laundering or financing terrorist activities. The updated regulatory framework also underscores the need to improve protections with respect to the personal data of European residents who have invested in crypto assets.

[1] *See* Press Release, "Crypto Assets: Deal on the New Rules to Stop Illicit Flows in the EU" European Parliament (June 29, 2022), here.

Compliance Obligations Imposed by Proposed Rule Updates

As a general matter, the proposed updates to the EU Travel Rule require a financial institution, when transferring funds, to pass on certain information to the receiving financial institution, thereby ensuring that information regarding the transaction is stored on both sides of the transfer. To be compliant, CASPs would be required to offer "full transparency and traceability" and store information regarding both the originator and beneficiary of a crypto transaction, including:

- The names of the payer and payee;
- The payer and payee's payment account numbers; and
- The payer's address, official personal document number, customer identification number, or date and place of birth.[2]

The obligation to maintain this information would apply to transfers between two CASPs or between a CASP and a financial institution, such as a bank, where at least one of the CASPs is established in the EU, and regardless of the value of the crypto assets involved in the transaction.[3] While the European legislators indicated that the proposed rule would not apply to person-to-person transfers, it would impose specific requirements for un-hosted wallets (e.g., wallet addresses held by private users) when they interact with hosted wallets managed by CASPs. Additionally, to improve the traceability of transfers of crypto assets, the proposed rule also requires the beneficiary CASP to implement adequate procedures and monitoring regarding the information received.[4] As such, European legislators made clear that the EU's General Data Protection Regulation ("GDPR"), "remains applicable to transfers of funds and that no separate data protection rules will be set up."[5] For many CASPs' current operations, which are built on the principle of anonymity, these new requirements are likely to present a new set of challenges.

Comparing the Updated EU Travel Rule with its U.S. Equivalent

The U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") maintains a similar rule, also known as the Travel Rule, that requires regulated financial institutions to transmit transaction and customer information to the next institution in the payment chain (i.e., ensure that the information "travels" to the receiving financial institution) for certain funds transfers and transmittals of funds. Under FinCEN's Travel Rule, the originator's bank or transmitter's

2 *Id.*; *See also* Regulation (EU) 2015/847 679 of the European Parliament and of the Council of 20 May 2015 on Information Accompanying Transfers of Funds and Repealing Regulation (EC) No 1781/2006, Article 4 here.

3 *See* Press Release, *supra* note 1.

4 *See* Press Release, "Anti-Money Laundering: Provisional Agreement Reached on Transparency of Crypto Asset Transfers" Council of the European Union (June 29, 2022) here.

5 *Id.*

financial institution is required to include certain information in the payment or transmittal order sent by the bank or nonbank financial institution to another bank or nonbank financial institution in the payment chain.[6] The Travel Rule requirements apply to CASPs to the extent they meet the definition of a financial institution; for example, because they are engaged in money transmission and therefore are a type of money services business regulated by FinCEN. In guidance, FinCEN has made clear that administrators and exchangers of virtual currency, among others, are generally considered money transmitters and are therefore subject to the Travel Rule and other Bank Secrecy Act-related requirements.[7]

In 2019, FinCEN advised that transactions involving convertible virtual currency ("CVC") qualify as a transmittal of funds and therefore may fall within the Travel Rule, if the other criteria for application of the rule are met.[8] In October 2020, FinCEN issued proposed rulemaking that would codify this guidance and explicitly apply the Travel Rule and corresponding recordkeeping requirements to applicable transactions involving CVC, as well as transactions involving digital assets with legal tender status, by clarifying the meaning of "money" as used in certain defined terms.[9]

While the EU's proposed amendment would apply to transfers within the scope of the rule regardless of the value of the crypto assets involved in the transaction, FinCEN's Travel Rule applies only to funds transfers and transmittals of funds in amounts of $3,000 or more (or its equivalent in CVC); however, there is pending rulemaking that would lower the threshold for the Travel Rule from $3,000 to $250 for international funds transfers and transmittals of funds.[10] This rulemaking has yet to be finalized.

Relatedly, in December 2020, FinCEN issued a Notice of Proposed Rulemaking that would (among other things) impose customer verification and counterparty identification requirements on banks and money services businesses -- including money transmitters involved in transfers of crypto assets -- for transactions with a value of $3,000 or more involving CVC held in un-hosted wallets.[11] This rulemaking has also yet to be finalized, and the feedback to the proposed rulemaking was overwhelmingly negative, meaning that there may be significant changes to the proposed rule prior to the publication of any future final rule.

6 The Travel Rule is codified at 31 CFR 1010.410(f)(1), and the corresponding recordkeeping requirements are codified at CFR 1020.410(a) (for banks) and 1010.410(e) (for nonbank financial institutions).

7 FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013) here.

8 FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 09, 2019) here. CVC is defined as a type of virtual currency that either has an equivalent value as currency or acts as a substitute for currency.

9 FinCEN Notice of Proposed Rulemaking (October 23, 2020) here.

10 *Id*.

11 FinCEN Notice of Proposed Rulemaking (December 23, 2020) here.

For CASPs in the EU and the United States, the Travel Rule requirements are part of a broader global effort to address the money laundering and terrorist financing risks posed by crypto assets.[12] These requirements pose a number of practical challenges related to data protection and security (as discussed below) and counterparty identification. Unlike traditional funds transfers between banks, where it is clear from the SWIFT messages whether the next institution in the payment chain is a regulated financial institution subject to the Travel Rule, the decentralized nature of cryptocurrency transactions means that it is not always clear whether the next entity in the payment chain is a regulated financial institution, and therefore, it is not always clear whether the Travel Rule even applies to the transaction. Without an industry-wide solution, it will remain difficult for CASPs to fully comply with the Travel Rule.

Data Protection and Security Challenges for CASPs

To date, most CASPs have not been required to treat crypto asset transfer-related customer information as personal data under applicable data protection laws, such as the GDPR.[13] Although it is still unclear how the proposed rule will specifically align with the requirements under GDPR, the compliance burdens for CASPs will likely increase significantly. For instance, the territorial scope of the GDPR applies to personal data processed by an entity (e.g., data controller or data processor) established in the EU, which is a requirement under the proposed rule for at least one of the transactional parties. Additionally, under the proposed rule, the originator CASP would be required to record the data identifiers previously noted above, which constitute personal data under the GDPR.[14]

While the goal of the regulation is to improve the detection of suspicious activities, the impact on CASPs' operations may be significant, depending on the maturity of the entity's data protection program. The data controller/data processor paradigm (as outlined under GDPR) is generally a challenging concept to apply directly to the context of a CASP, which, due to the decentralized nature of crypto asset transactions, may function as either a data controller or data processor, depending on the circumstance. As a result, CASPs may face a number of data protection considerations and challenges to take into account, including but not limited to, the following:

---

12 *See, e.g.*, Financial Action Task Force Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, *available* here.

13 *See* Personal Data Protection Commission, Singapore, "Guide on Personal Data Protection Considerations for Blockchain Design," page 16. (Recent guidance disseminated by Singapore's data protection authority, the Personal Data Protection Commission ("PDPC"), offers considerations and recommendations for both permission-based and permissionless networks to be designed to achieve compliance with Singapore's Personal Data Protection Act. The PDPC document addresses similar data protection issues as those addressed under GPDR, including data retention, technical and organizational controls, and data controllership. With respect to permissioned networks, the PDPC advises that entities implement the following measures: (1) admitting only participants with comparable standards of data protection; (2) requiring encryption of personal data on-chain; and (3) monitoring and enforcing against any personal data breaches on the network.)

14 *See* Legislative Proposal, *supra* note 2.

- Data Subject Rights. Individuals who have provided their personal data to CASPs maintain a host of rights under GDPR, including the rights to access, transmit (e.g., portability), restrict processing, correct, and delete their personal data. Fulfilling these obligations will likely be challenging, particularly if the personal data associated with transactions is recorded on-chain. By design, any deletion or modification is extremely difficult due to the immutable nature of the blockchain. For instance, generally, a request from a data subject to have his or her wallet and/or transaction history deleted on-chain would be impossible to fulfill without at least 51% control of the network by the CASPs.[15]

- Data Retention. The personal data identifiers of EU individuals collected by CASPs will be subject to data retention requirements under GDPR, which obligate them to keep data no longer than necessary for the purpose for which data is processed.[16] As a result, CASPs should consider drafting data retention policies for any personal data that is maintained on their systems and should implement secure data storage solutions.

- Data Minimization. Under GDPR principles, personal data processing must be limited to only what is necessary in relation to the purpose for which the personal data is processed.[17] In order to comply with the principle of data minimization, any data identifier collected by a CASP in furtherance of a transaction should be limited solely to what is prescribed under the proposed rule.

- Data Protection by Design. The concept of "data protection by design and by default" includes incorporating data protection considerations into the technology's development stage. Under GDPR, this includes taking into account the "state of the art, the cost of implementation and the nature, scope, context, and purposes" of how personal data is processed, as well as other factors such as the amount of data collected and the retention periods.[18] For CASPs, the practical effect means that when developing crypto asset-based platforms or services, developers and technologists must incorporate privacy considerations into their design before beginning processing operations, including by considering whether personal data may be stored off-chain.

- Data Protection Impact Assessments ("DPIAs"). Where any new technology is contemplated or where the processing of personal data based on automated processing may result in decisions that produce legal effects on individuals, organizations must carry out an assessment, or DPIA, that identifies and addresses the risks inherent in that processing. A DPIA may be undertaken in coordination with and on the advice of a data protection

---

15 *See* Binance Academy, "What is a 51% Attack?" (updated, April 5, 2022) here.

16 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 5(1)(e)

17 *Id.* at Article 5(1)(c).

18 *Id.* at Article 25(2).

officer.[19] In particular, for CASPs, this evaluation may consider a description of how personal data is processed, how that processing may affect the rights of a data subject, and performing a risk assessment of the safeguards used to protect personal data.[20] It is unclear whether crypto asset transaction technology might be considered new technology or at what point crypto asset transactions might be considered high-risk processing.

- Cross-Border Data Transfer. Under GDPR, personal data may only be transferred outside of the EU when adequate safeguards are available in the jurisdiction to which the personal data is transferred or subject to approved data transfer mechanisms such as standard contractual clauses. However, the distributed nature of blockchain technology is at odds with the GDPR's restrictive approach to cross-border data transfers. On a blockchain, every block of data or node has a copy of all the data stored in the ledger, and as such, any personal data in that ledger flows freely to and from each node regardless of localization or jurisdictional concerns. Transfers to countries that have not been found to maintain "adequate" protections, including the United States, must be made in a manner that satisfies the GDPR's requirements.

- Data Security. In assessing data security (e.g., appropriate encryption, pseudonymization measures, and access controls), an entity must implement technical and organizational measures to ensure the level of protection provided is appropriate to the risk.[21] Similarly, under GDPR data integrity principles, personal data must be secured and protected from unauthorized or unlawful processing and against accidental loss, destruction, or damage.[22] For CASPs, safeguarding the data security of crypto assets transactions and the identity of the wallet holder is crucial to lowering the risk of exposing customer personal data in the event of a data breach. Notably, the proposed rule raises security concerns for both CASPs and their customers because it would mandate the generation of a database of information capable of associating the individual and wallet address behind each transaction. Such a database would naturally become an appealing target for cybercriminals. Without robust security measures, CASPs could expose their users to significant security threats. In addition, data security implications are a particularly important consideration for EU CASPs when assessing the compliance challenges of dealing with non-EU CASPs that are not subject to the requirements of the proposed rule.

[19] *Id.* at Article 35(2).

[20] *Id*. at Article 35(7).

[21] *Id*. at Article 32(1).

[22] *Id*. at Article 5(1)(f).

The proposed revisions to the EU Travel Rule are anticipated to come into effect in July 2024, giving CASPs almost 24 months to navigate design constraints and bring their privacy and data security practices to the level of data protection maturity required by the GDPR.[23]

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Britt Mosman
202 303 1057
bmosman@willkie.com

Nikki M. Cronin
650 887 9327
ncronin@willkie.com

Kari Prochaska
312 728 9080
kprochaska@willkie.com

Amal Ibraymi
212 728 3524
aibraymi@willkie.com

[23] *See* European Commission, "Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions – On a Digital Finance Strategy for the EU" COM (2020) 591 (September 24, 2020); *See also*, "Guide on Personal Data Protection Considerations for Blockchain Design," *supra* note 14, at 22-23.