



To:

Secretariat of the Financial
Action Task Force (**FATF**)

2 Rue André Pascal, 75116
Paris, France

*Submitted via email at
FATF.Publication@fatf-gafi.org*

April 18, 2025

**Re: Second Public Consultation on Recommendation 16 on
Payment Transparency**

Coinbase Global, Inc. (together with its subsidiaries, **Coinbase**) thanks the Financial Action Task Force (FATF) for soliciting feedback on the proposed revisions to FATF Recommendation 16 (R.16).

Coinbase is the most trusted crypto trading and custody platform in the world. Founded in 2012 in the United States and publicly listed on the NASDAQ in 2021, we have grown to serve millions of verified retail and institutional investors across the world, offering a secure and user-friendly interface for both. We are committed to building an open financial system for the world and operate with strong regulatory compliance, security protocols, and innovative features to ensure a seamless and trustworthy user experience. The practices developed at Coinbase provide useful insights that inform our comments.

We recognize that FATF serves as a pillar of global financial security, coordinating international efforts to combat money laundering, terrorist financing, and threats to the financial system's integrity. Through its rigorous standards and comprehensive evaluations, FATF has fostered cooperation among nations, financial institutions, and law enforcement agencies worldwide, strengthening regulatory frameworks and enhancing transparency across global financial networks to safeguard economic wellbeing.

In striking the right balance between payment transparency and privacy, cybersecurity, and other operational considerations, we encourage FATF to reconsider two of the proposed changes to R.16, which would expand the scope of sensitive personal information that financial institutions must collect and share. We believe the negative consequences of the proposal outweigh the potential benefits.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Faryar Shirzad".

Faryar Shirzad
Chief Policy Officer

Our views on the proposed changes to Recommendation 16

FATF Recommendation 16 and its accompanying Interpretive Note (together, R.16) concern the Travel Rule, describing when and how it applies to financial institutions (FIs) who provide value transfers. Through this consultation, FATF is proposing to amend which categories of Travel Rule information (about the originators and beneficiaries of value transfers) FIs must collect and transmit to one another. Although R.16 does not directly apply to virtual asset service providers (VASPs), it indirectly applies to VASPs via FATF Recommendation 15 and its Interpretive Note (together, R.15), which state that countries should apply certain FATF recommendations, including R.16, to VASPs such as Coinbase. Thus, we recommend that FATF reconsider its proposal to expand the scope of mandatory Travel Rule information to include (1) the originator's date and place of birth; and (2) the beneficiary's address.

R.16 should not require collection of the originator's date and place of birth

As a regulated VASP committed to Anti-Money Laundering ("AML") and Countering the Financing of Terrorism ("CFT") compliance, we strongly urge FATF to reconsider the proposed amendment to R.16 *requiring* that the information accompanying qualifying cross-border transfers *always contain* the originator's date of birth (DOB) and place of birth (POB).¹ While we support the Travel Rule's objectives, these specific requirements create disproportionate risks relative to their benefits.

While most VASPs are required to collect identifying information about their customers as part of their Know Your Customer/Customer Due Diligence ("KYC"/"CDD") obligations, the proposed POB/DOB requirement counterproductively threatens to expand KYC/CDD requirements beyond current legal standards. While some jurisdictions today may require FIs to collect a person's POB as part of the customer onboarding application, many others, such as the United States, do not. The current version of R.16 appropriately recognizes and accommodates these cross-border differences; it provides that FIs *may* collect and share an originator's POB and DOB, but it also allows FIs to use alternative data points, such as the originator's national identity or customer identification number. By contrast, the proposed revision to R.16 does not account for these nuances. Instead of empowering FIs to adopt a risk-based approach tailored to their existing, local legal obligations, it would impose a blanket POB/DOB requirement on FIs throughout the world. Thus, this proposal would exacerbate the "Sunrise Issue" that currently plagues global Travel Rule compliance, placing VASPs in the difficult position of either adhering to their local KYC/CDD obligations or engaging in value transfers that do not align to FATF recommendations.

Further, revising R.16 to require POB and DOB information may lead to unintended consequences that disproportionately impact vulnerable populations around the world. Whether due to conflict, natural disasters, or other factors, inter- and intra-national borders are subject to change, meaning that birth records may be scarce, inaccurate, or not aligned to anglicized geographical markers. Moreover, refugees, asylum seekers, and politically marginalized individuals may not be able to provide this information to FIs, even if they can provide other identifying information. Requiring POB and DOB information to be collected (and shared) in order to conduct value transfers does not account for these

¹ Where the originator is a natural person.

practical constraints, and thus it risks ostracizing many of the communities that virtual assets are intended to reach and empower. Once again, this poses a significant dilemma for VASPs: either deviate from these new FATF standards or else restrict transfers for these vulnerable individuals, effectively debanking them. And although we appreciate FATF's comment in this consultation that steps *should* be taken to avoid financial exclusion, we respectfully submit that a more effective approach would be to retain R.16's *current*, more nuanced approach to POB and DOB collection, which is more sensitive to geopolitical realities.

Additionally, requiring the collection and transmission of DOB and POB will raise significant privacy concerns for VASPs and the users who rely on them to interact with the financial system. These personal identifiers, when combined with other required information under R.16, create comprehensive profiles that could become significant targets for cyber criminals and other bad actors, enabling widespread identity theft if the records were compromised. Further, in many jurisdictions (and for self-evident reasons) date and place of birth are considered sensitive personal data subject to stringent protection under frameworks like GDPR and CCPA, potentially creating conflicts for FIs required to satisfy privacy and security requirements on the one hand, and Travel Rule obligations on the other.

Similarly, from a cybersecurity perspective, the proposed requirements would expand the attack surface for VASPs and the entire virtual asset ecosystem. The transmission of additional personally identifiable information across multiple entities increases the likelihood and potential impact of data breaches. And once compromised, date and place of birth information cannot be changed—unlike passwords or other credentials—creating *permanent* vulnerabilities for victimized users.

Operationally, implementing these new requirements would also necessitate significant modifications to existing Travel Rule compliance systems, and at substantial cost. Many VASPs have only recently completed their implementation of current R.16 requirements, and this change would require rebuilding messaging protocols, updating compliance software, and retraining staff. The increased data collection would also create friction in legitimate transactions, potentially driving users to non-compliant VASPs or peer-to-peer exchanges outside of regulatory oversight.

We firmly believe that effective AML/CFT measures must balance whatever benefits they may bring in combatting illicit finance against privacy, data protection, and other key considerations. The current version of R.16 already enables sufficient identification and monitoring of value transfers. We therefore recommend maintaining the existing Travel Rule requirements without these additions while continuing industry-regulator dialogue to develop more balanced approaches to combating illicit finance in the virtual assets ecosystem.

R.16 should not require collection of the beneficiary's address

The proposed amendment to R.16 would also newly require VASPs to collect sensitive address information about their customers' counterparties—specifically, the address of the beneficiary of a value transfer—then transmit that information to the counterparty

VASP. This should be reconsidered, as it raises serious privacy concerns yet provides questionable returns in terms of combatting illicit finance.

Ultimately, requiring VASPs to collect a beneficiary's address provides limited benefits—to regulators, law enforcement, or VASPs' compliance staff—due to data reliability issues. For entirely legitimate reasons, a VASP's customer will not know their counterparty's address or be unwilling to divulge such sensitive information, leading to high failure rates. Customers may also inadvertently provide VASPs with inaccurate information, undermining compliance efforts by feeding bad data into AML/CFT screening protocols. Under these circumstances, imposing an affirmative duty on a VASP to collect and share beneficiary address information is thus counterproductive to R.16's overarching goal of increasing transparency.

Additionally, a large percentage of the world's population does not have an address that VASPs could collect or share. Per United Nation estimates, as many as four billion people live in places without street names and/or numbers. Addresses, while common in the developed world, prove to be a barrier for financial services for many throughout the developing world. If VASPs were to require a beneficiary address before processing a transaction, it would eliminate the possibility of processing payments to people without an address—often, the people who need it the most.

As Coinbase's mission statement is to increase economic freedom in the world, it opposes the administrative burden that this proposal would entail, as well as the debanking effect it would have. Virtual asset payments are uniquely designed for empowering marginalized communities, whether it is sending micro-payments to women for work in countries where they cannot have bank accounts, or donations to non-profits operating across borders or in places without formal municipal infrastructure. Requiring the collection and transmission of the beneficiary address will force Coinbase and other VASPs to curtail transactions to those that need the blockchain-based payment infrastructure the most.

However, even if this information *could* be readily gathered, the proposed revision to R.16 would dramatically increase the amount of personal data that VASPs collect, store, and share, requiring them to gather information on third parties who neither chose to be a customer of that VASP nor agreed to any terms covering the use of their data—and may not even realize their data is being collected and stored in the first place. This is in stark contrast to how VASPs normally obtain sensitive personal information. When Coinbase, for example, collects data from its own customers, it does so after they voluntarily agree to a disclosed privacy policy and terms of use. By contrast, non-customer counterparties have not agreed to anything with respect to their data.

The scale of this proposed expansion in financial data monitoring is significant, turning VASPs into involuntary custodians of massive amounts of non-customer data. Perhaps for this reason, policymakers who oversee some of the world's largest economies—such as the United States, European Union, India, United Kingdom and others—have declined, when enacting their own Travel Rule regulations, to require the collection and transmission of beneficiary address information. We encourage FATF to follow their approach and retain the current version of R.16, which better accounts for these many risks.

Conclusion

In addition to the recommendations above, we would encourage FATF to clarify to AML/CFT regulators that the proposed R.16 revisions—if adopted despite the concerns discussed above—would not directly extend to VASPs and that current compliance expectations would instead remain aligned with R.15. We also encourage FATF to solicit additional input from VASPs and crypto industry trade associations to identify how R.15 should be interpreted and applied in light of the final updates to R.16.