

# CONSULTATION FEEDBACK NOTE

Relating to Directive 9 on the implementation  
of the “Travel Rule” relating to crypto asset  
transfers in accordance with the Financial  
Action Task Force Recommendations

**15 November 2024**

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
1.	<p><b>De minimus threshold for crypto asset transfers</b> – various views include -</p> <ul style="list-style-type: none"> <li>• The advocating for a zero threshold – reason being that it is fair and reasonable to apply a zero threshold on crypto asset transfers for Travel Rule obligation, which is a popular regulatory approach from many regulators around the world including the European Markets in Crypto-Assets Regulation (MiCA).</li> <li>• That the <b>threshold</b> applied should be in line with the FATF <i>de minimus</i> threshold of USD 1000 or EUR 1000. Further, that applying a threshold above zero strikes a balance between regulatory vision with practicality and fairness. Implementing the Travel Rule for all transactions can be costly for CASPs, especially smaller ones.</li> <li>• Proposal that to ensure consistency the threshold should be aligned with the Directive that was issued by SARB (Directive 1/2022) regarding electronic funds transfers i.e. set a threshold of R10 000.</li> </ul>	<ul style="list-style-type: none"> <li>• Note the advocating of a zero threshold and note the arguments for this.</li> <li>• The decision taken is that in the final Travel Rule Directive, the <i>de minimus</i> threshold in respect of a business relationship is zero. Para 2.1.9 of the final directive takes this into account by defining a “qualifying transfer”.</li> <li>• The crypto assets market is known for its volatility. Setting a <i>de minimus</i> threshold above zero will be difficult to monitor – and supervision of this aspect in the implementation of the travel rule becomes difficult.</li> <li>• Financial inclusion is not an issue to be taken into account here – it is an issue to be considered in the remittance market.</li> <li>• Most commentators confused the R5 000 <b>single transaction threshold</b> (paragraph 4.6 in the draft Travel Rule Directive) with a <i>de minimus</i> threshold.</li> </ul>
2.	<p><b>Crypto asset transfers to or from an unhosted wallet</b> - A range of comments were received, however, most commentators advocated for a flexible risk-based approach and agreed that para. 8 of the draft Directive is sufficient.</p> <ul style="list-style-type: none"> <li>• One commentator recommends the requirement for all unhosted wallets to be screened against the US Treasury’s Office of Foreign Assets Control (OFAC) Special Designated National (SDN) list, and any other appropriate sanctions lists before a received crypto asset transfer is</li> </ul>	<ul style="list-style-type: none"> <li>• For the most part, para. 8 kept as is</li> <li>• There are FIC Act obligations for accountable institutions to screen against UN Security Council sanctions list, not the OFAC list. However, it is up to the accountable institution to decide if they wish to screen against a list such as OFAC.</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	credited to the customer’s account or transferred out of the account.	
3.	<p><b>Crypto asset transfers to or from other crypto asset service providers and counterparty crypto asset service provider identification and due diligence – para 4.8 of the Draft Directive – various view from commentators -</b></p> <ul style="list-style-type: none"> <li>• Agree with the content set out in paragraph 4.8 of the draft. Observed that counterparty due diligence has been an effective regulatory tool in mitigating AML/CFT risks in the crypto asset industry.</li> <li>• Agree that if the originator CASP is not able to conduct CDD on the counterparty CASP then the originator should not proceed with the transaction in line with section 21E of FICA (inability to conduct CDD).</li> <li>• Advised that the requirement to perform due diligence on counterparty CASPs is necessary, however, the provision within paragraph 4.9, specifically the requirement that a transaction should not proceed in the event that conducting due diligence is not possible, is impractical. The cryptocurrency market is known for its volatility and rapid changes. Para 4.9 – places an unreasonable burden on the originating institution.</li> <li>• Commentator suggests doing away with due diligence requirements for transactions involving only local, licensed crypto asset service providers (except for confirmation of the license’s standing) should no other risk flags be triggered for a transaction. The rationale behind this approach is</li> </ul>	<ul style="list-style-type: none"> <li>• Keep para 4.8 (para 4.7 in the final directive) as is.</li> <li>• Keep para 4.9 (para 4.8 in the final directive). No point in having para 4.8 if we cannot include para 4.9.</li> <li>• It is not unreasonable to expect a CASP to conduct counterparty due diligence on the CASPs that they will be/are dealing with/conducting crypto transactions on behalf of their clients.</li> <li>• The paragraphs on counterpart due diligence in the Travel Rule Directive is in line with the FATF Updated Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers (2021) – <a href="https://www.fatf-gafi.org/publications/virtualassets/Pages/Updated-Guidance-for-a-Risk-Based-Approach-for-Virtual-Assets-and-Virtual-Asset-Service-Providers.aspx">Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org)</a> . Information as set out in paragraph 196 of the FATF Guidance – For a VASP to transmit required information to another VASP, however, it is necessary for them to identify their counterparty VASP. A VASP would also need to conduct due diligence on their counterparty VASP before they transmit the required information to avoid dealing with illicit actors or sanctioned actors unknowingly...Considering the concept of due diligence, countries should expect a VASP to refresh their counterparty due diligence information periodically or when risk emerges from the relationship in line with their defined RBA control structure...VASPs should use this due diligence process to determine whether a counterpart can reasonably be expected to protect the confidentiality of information shared with it.</li> <li>• Due diligence requirements will be required for all CASPs, whether locally licensed or located abroad. The manner and extent to which such due diligence is conducted on local CASPs and international CASPs will be documented in an accountable institution’s risk management and compliance programme (RMCP). Paragraph 4.10 of the draft Travel Rule Directive does state that “An ordering crypto asset service provider must provide for the manner in which and the processes by which it will implement measures to comply with the requirements of paragraphs 4.1 to 4.9 above, in the risk management and</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	<p>that local regulator already maintains sufficient oversight of the legitimacy of these entities.</p> <ul style="list-style-type: none"> <li>• The Directive should specify what constitutes adequate due diligence in relation to counterparty CASPs. This includes defining the scope and depth of due diligence required, such as verifying the regulatory status of the counterparty, understanding their ownership and control structure, and assessing their AML/CTF policies.</li> <li>• Agrees that due diligence should be conducted on counterparty CASPs, but does not agree with the requirement that a CASP must ascertain whether a counterparty CASP will be able to keep the information confidential. This requirement is too vague to comply with practically. How would a CASP satisfy itself that this requirement will be met?</li> </ul>	<p>compliance programme that the ordering crypto asset service provider is required to develop, document, maintain and implement in accordance with section 42 of the FIC Act.”</p>
4.	<p><b>Sunrise issue</b> Comments included concerns –</p> <ul style="list-style-type: none"> <li>• Imposing stringent requirements on interactions with jurisdictions that have not yet adopted the travel rule could isolate South Africa from vital regional transactions. Instead, South Africa should lead by example and encourage compliance without severing financial links.</li> <li>• Imposing stringent requirements for travel rule compliance between cross-border transactions would be a massive impediment to local industry.</li> <li>• The Directive should ease certain requirements of the Travel Rule for interactions between CASPs in compliant jurisdictions and their counterparts in jurisdictions that have not yet implemented the Travel Rule.</li> </ul>	<ul style="list-style-type: none"> <li>• The FIC and the FATF understand the challenges in implementing the travel rule for crypto asset transactions, however, it is imperative that jurisdictions globally implement this FATF standard to ensure transparency in crypto asset transactions.</li> <li>• CASPs must send the travel rule information to CASPs even if they are in jurisdictions where the travel rule is not yet implemented.</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	<ul style="list-style-type: none"> <li>Commentators also recommend that the Directive include measures allowing CASPs to be flexible and follow a risk-based approach in line with FICA’s principles.</li> </ul>	
5.	<p><b>Privacy coins</b> Comments included the support for the prohibition of the use of privacy coins while others argued for allowing the use of privacy coins based on a risk-based approach –</p> <ul style="list-style-type: none"> <li>Believe that privacy coins or AECs (Anonymity-Enhanced Cryptocurrencies) should be prohibited - recommend zero-tolerance as it poses unjustifiable risks. Advise that in reality, there isn’t much commercial justification to allow facilitation of AECs.</li> <li>In line with section 20 of FICA (anonymous/false/fictitious name) the directive should prohibit the use of privacy coins in crypto asset transactions. In the spirit of AML/CFT/CPF transparency in respect of transactions is critical.</li> </ul> <p>While on the other end of the spectrum some commentators argued as follows -</p> <ul style="list-style-type: none"> <li>Use of privacy coins should not be prohibited. Allowing the use of privacy coins acknowledges the legitimate use cases for enhanced privacy, such as protecting users from identity theft or safeguarding sensitive financial information.</li> <li>Rather than imposing a ban on the use of privacy coins in crypto asset transactions in the Directive, CASPs should adopt a risk-based approach as to whether to offer privacy coins.</li> <li>Rather than automatically reporting all transactions involving privacy coins as</li> </ul>	<ul style="list-style-type: none"> <li>Most commentators seem to argue for allowing the use of privacy coins based on a risk-based approach.</li> </ul> <p>FATF VA / VASPs Guidance (2021) referred to above - Supervisors should give priority to the potential areas of higher risk, either within the individual VASP (e.g., to the particular products, services, or business lines that a VASP may offer, such as particular VAs or VA services like AECs.</p> <p>The FIC notes that the Travel Rule Directive is not the correct place to prohibit privacy coins. In addition, by prohibiting the use of privacy coins this may have unintended consequences.</p>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	<p>suspicious, the directive could stipulate conditions under which such transactions must be reported.</p>	
6.	<p><b>Privacy concerns</b> – comments included –</p> <ul style="list-style-type: none"> <li>• The implementation of the Travel Rule in South Africa presents significant privacy challenges, particularly relating to the Protection of Personal Information Act (POPIA). POPIA places restrictions on the transfer of personal information outside South Africa, permitting such transfers only to countries that offer similar levels of data protection. The global nature of cryptocurrency transactions, however, means personal data may need to be transmitted to entities in countries that do not have equivalent privacy safeguards, potentially violating POPIA.</li> <li>• The principle of data minimization in POPIA dictates that only the data necessary for achieving a specified purpose should be collected and processed. The implementation of the Travel Rule could conflict with this principle by necessitating the collection of extensive personal information for each transaction above a certain threshold, which might not always be strictly necessary for completing the transaction itself.</li> </ul>	<ul style="list-style-type: none"> <li>• The processing of personal information of clients for the purposes of the FIC Act compliance may only be done within the confines of the Protection of Personal Information Act, 2013 (the POPI Act). The processing and further processing of personal information of a client for purposes of FIC Act requirements is allowed in terms of the POPI Act. Refer to Guidance Note 7 – <a href="#">2017.10-Guidance-Guidance-Note-7-FIC-Act-obligations.pdf</a></li> <li>• Accountable institutions should take the necessary steps to ensure that the CASPs they are dealing with offer the necessary safeguards in relation to their client’s personal information, when they conduct the counterpart due diligence.</li> <li>• The Travel Rule Directive is based on the FATF standards and guidance. The information sought in respect of the originator client and beneficiary client is in line with the FATF standards, is necessary for the transparency of crypto asset transactions, and it is not extensive information that is being sought.</li> </ul>
7.	<p>Comment - proposes the introduction of an explicit requirement for the recipient CASP to verify that the beneficiary information received from the ordering CASP matches the information verified during its customer due diligence procedures. Noting that the FATF is considering</p>	<ul style="list-style-type: none"> <li>• From the FATF Rec 16 consultation paper – <i>When and how the R.16 revision applies to the virtual assets (VA) sector will be considered separately by FATF.</i> Further, it is premature to draft the Travel Rule Directive taking into account FATF’s consultative work on Recommendation 16, which is still ongoing, and may possibly be finalised during the course of 2025.</li> </ul>

<b>COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS</b>		
<b>NO.</b>	<b>COMMENTS RECEIVED</b>	<b>FIC RESPONSE</b>
	the introduction of this requirement as part of the ongoing revision of Recommendation 16.	
8.	<ul style="list-style-type: none"> <li>Section 2.1.3 defines a ‘domestic transfer’ as one where both CASPs are located in South Africa. It should be noted that many ‘local’ CASPs use international trading platforms for their settlement and liquidity systems. This may only be a technical matter, however, commentator recommends that this is clarified for the industry.</li> </ul>	<ul style="list-style-type: none"> <li>Clarify further in guidance</li> <li>The location of international trading platforms is irrelevant in the implementation of the travel rule directive.</li> </ul>
9.	<ul style="list-style-type: none"> <li>Commentator recommends that updates are made to the definitions given in paragraphs 2.1.6 and 2.1.8 and/or the definition in paragraph 2.1.2 in order to clearly apply travel rule requirements to cross border crypto asset transfers.</li> </ul>	<ul style="list-style-type: none"> <li>Edits made through the final directive to make this clearer</li> </ul>
10.	<ul style="list-style-type: none"> <li>Commentator states that it appears only accountable institutions listed in items 12 and 22 of Schedule 1 to the FIC Act can be ordering or recipient CASPs. Accountable Institutions under Item 12 does not facilitate or enable the origination or receipt of domestic and cross-border transfers of crypto assets or act as an intermediary in receiving or transmitting the crypto assets for or on behalf of a client, but offers financial advice or intermediary services in respect of crypto assets.</li> </ul>	<ul style="list-style-type: none"> <li>Yes, only these accountable institutions (item 12 Crypto FSPs; and item 22 CASPs) that engage in crypto asset transfers. In October 2022 the FSCA designated a crypto asset as a financial product under the Financial Advisory and Intermediary Services Act, 37 of 2002. Any person who provides any advice or intermediary services as a business in respect of crypto assets, must be licensed by the FSCA. ‘Intermediary service’ as defined in the FAIS Act is wide enough to cover, among other, the buying, selling or otherwise dealing in (whether on a discretionary or non-discretionary basis) of crypto assets. The directive on the travel rule is aimed at those entities that, as a business, engage in crypto asset transfers for or on behalf of a client and falls under items 12 and/or 22 of Schedule 1 of the FIC Act.</li> </ul>
11.	<ul style="list-style-type: none"> <li>Commentator advises that “qualifying transfer” is not defined in the Directive - recommends that a definition is included to provide stakeholders with certainty as to which transfers are in scope.</li> </ul>	<ul style="list-style-type: none"> <li>“qualifying transfer” defined in the final directive</li> </ul>
12.	<ul style="list-style-type: none"> <li>Proposes that the obligation to transmit the originator’s wallet address (4.1.3.3) be broadened to include an originator’s account number or</li> </ul>	<ul style="list-style-type: none"> <li>Edits considered – relevant paragraphs re-drafted</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	<p>unique transaction reference number (should an account number not be available).</p>	
13.	<ul style="list-style-type: none"> <li>Should additional information, as provided for in 4.1, be obtained and transmitted in respect of a cross-border transfer that is a single transaction more than R5,000.</li> </ul>	<ul style="list-style-type: none"> <li>Para 4.6 and 4.7 (of the draft directive) refer to the single transaction threshold of R5 000. Yes – additional information must be obtained and transmitted in respect of a cross-border transfer that is a single transaction of more than R5 000.</li> </ul>
14.	<ul style="list-style-type: none"> <li>Whether the requirements outlined in paragraph 4.1, pertaining to obtaining and transmitting ID Number or Passport number and Address or place of birth, should be included in respect of a cross-border transfer that is a single transaction of less than R5,000. Or should this section be read as an exception to the provisions of 4.1 only in the case of a single cross-border transaction under the prescribed threshold?</li> </ul>	<ul style="list-style-type: none"> <li>No – para 4.6 of the draft directive states the information in respect of a cross-border transfer that is a single transaction of less than R5 000, the ordering crypto asset service provider must transmit to the recipient crypto asset service provider. Para 4.7 of the draft directive states that an ordering crypto asset service provider need not verify the information referred to in paragraph 4.6 in respect of a cross-border transfer that is a single transaction valued at less than R5 000 for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the ordering crypto asset service provider must verify the information pertaining to the originator.</li> </ul>
15.	<ul style="list-style-type: none"> <li>Paragraph 4.1- the requirement to obtain and verify the residential address may not always be readily available as many CASP’s only obtain and verify this information for higher risk clients.</li> </ul>	<ul style="list-style-type: none"> <li>Para 4.1.3.1 requires the originator’s residential address, <b>if such an address is readily available</b>, the residential address is not mandatory. If that information (residential address) is available, then provide it, or else provide the alternate information requested.</li> </ul>
16.	<ul style="list-style-type: none"> <li>Para 4.1.3 - From a screening perspective, a wallet address while important for identification purposes will not aid the screening and management of results thereof. Suggest “country of residence” be used to replace residential address.</li> </ul>	<ul style="list-style-type: none"> <li>Re-draft in the final directive – para 4.2.1</li> </ul>
17.	<ul style="list-style-type: none"> <li>There appears to be some conflict between the requirements of section 4.2 and section 4.7 in respect of verification of information. It is the commentator’s view that the provisions of section 4.7 should take precedence, where the</li> </ul>	<ul style="list-style-type: none"> <li>There is no conflict between para 4.2 and 4.7. Para 4.2 refers to transactions that are not a single transaction. Para 4.7 refers to transactions that are a single transaction. Most commentators confused the single transaction threshold in para 4.7 of the draft Directive with a <i>de minimus</i> threshold.</li> </ul>



COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS		
NO.	COMMENTS RECEIVED	FIC RESPONSE
	transaction value is less than the threshold (R5,000 currently proposed in the draft Directive).	Refer to GN 7 for further guidance on the single transaction – The FIC Act defines a single transaction as a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5 000 (the amount is determined by the Minister of Finance in the Regulations). This can be described as occasional or once-off business where there is no expectation on the part of the accountable institution or the client that the engagements would recur over a period of time.
18.	<ul style="list-style-type: none"> <li>Commentator requires clarification /amendments to the phrase “all information” in paragraph 4.3. Assume that so long as an ordering CASP fulfils its obligations in paragraph 4.1, then that would be sufficient. Same comment applies to para 4.5. Recommend that 4.3 be amended to specifically reference “all information pertaining to the wallet <u>as required in 4.1</u>” (underlined insertion).</li> </ul>	<ul style="list-style-type: none"> <li>Edits made in the final directive</li> </ul>
19.	<p><b>Para 5 – Obligation of Intermediary crypto asset service providers</b> – comments included -</p> <ul style="list-style-type: none"> <li>This requirement may not necessarily be applicable, depending on the nature and involvement of the intermediary CASP (e.g. the intermediary CASP’s role may be limited to a certain function but it is not actually involved in the transfer and transmission of crypto assets). To avoid unintended consequences, can the FIC consider narrowing this to apply to intermediary CASPs who are directly involved in the transaction and transmission chain.</li> <li>Para 5.3 - An intermediary crypto asset service provider must develop, document, maintain and implement effective risk-based policies and procedures for determining: 5.3.2 the appropriate follow-up action that the intermediary crypto asset service provider will take in each instance where it executes, rejects or suspends a cross-border</li> </ul>	<ul style="list-style-type: none"> <li>Keep drafting – this is in line with the FATF <i>Updated Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers – Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org)</i> Refer to paragraph 202 of the FATF guidance...Countries should ensure that such intermediary institutions (whether a VASP or other obliged entity) also comply with the requirements of Recommendation 16, as set forth in INR. 15, including the treatment of all VA transfers as cross-border qualifying transfers. Just as a traditional intermediary FI processing a traditional fiat cross-border wire transfer must ensure that all required originator and beneficiary information that accompanies a wire transfer is retained with it, so too must an intermediary VASP or other comparable intermediary institution that facilitates VA transfers ensure that the required information is transmitted along the chain of VA transfers, as well as maintaining necessary records and making the information available to appropriate authorities upon request.</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	<p>crypto asset transfer referred to in paragraph 5.3.1 above - Can the FIC provide clarity on what is intended by 5.3.2 and the envisaged end-result? For example, would this mean that an intermediary CASP would need to return the funds to the ordering CASP?</p>	
20.	<ul style="list-style-type: none"> <li>• The FIC has not provided clear guidelines or directives on how domestic crypto asset transfers should be treated. This regulatory uncertainty can stifle innovation and create compliance challenges for CASPs.</li> </ul>	<ul style="list-style-type: none"> <li>• The travel rule directive covers both domestic and cross-border crypto asset transactions. It is important to note that in effecting the obligations in the travel rule directive, CASPs remain obliged to also comply with any other applicable legislation involving crypto assets and participants should obtain independent legal advice in this regard.</li> </ul>
21.	<ul style="list-style-type: none"> <li>• Para 4.1 - As per the FATF’s guidance in October 2021, it was recommended that originator information should include: <ul style="list-style-type: none"> <li>• The name of the originator</li> <li>• The account number / wallet address; and</li> <li>• One of the following: <ul style="list-style-type: none"> <li>○ Physical address</li> <li>○ National identity number</li> <li>○ Customer identification number</li> <li>○ Date and place of birth</li> </ul> </li> </ul> <p>Given the general concerns over data privacy and security as well as the administrative burden on CASPs, commentator proposes that clause 4.1 be amended to align to the above guidance from FATF in order to mitigate the risks faced...</p> </li> </ul>	<ul style="list-style-type: none"> <li>• Taking into account FATF guidance, the Travel Rule Directive is drafted in a manner that will make sense in the South African context</li> </ul>
22.	<ul style="list-style-type: none"> <li>• Para 6.4.1 - Due to the nature of crypto asset transactions and the ability generally for a person or entity to send crypto assets to any wallet freely, it is not feasible for a recipient CASP to “reject” a transfer as the crypto asset, once confirmed on the blockchain, will be in the</li> </ul>	<ul style="list-style-type: none"> <li>• Final directive edited taking comment into account</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	<p>recipient wallet address. Commentator proposes that the “rejection” wording is removed from this clause.</p> <ul style="list-style-type: none"> <li>• Para 6.3 - The principle behind the detail required in 4.1 is that you cannot process a transaction without all the details verified, otherwise you must return the transaction. Therefore, it is not correct to do post-event monitoring even though it is provided for by the FATF as the information in 4.1 is expected to flow simultaneously.</li> </ul>	
23.	<ul style="list-style-type: none"> <li>• Also propose the deletion of “financial Institution” from the definition, as a financial institution would be required to register as a CASP if they perform the activities in item 22(c) conducting a transaction that transfers a crypto asset from one crypto asset address or account to another.</li> <li>• Paras. 4.1.3, 4.1.3.1- The qualification of “if such an address is readily available” is not used in FATF. If the address cannot be verified by the KYC processes of the ordering CASP then one of the other options must be used.</li> </ul>	<ul style="list-style-type: none"> <li>• With respect to “financial institution”, final directive edited</li> <li>• “Readily available” is a term used in FIC Money Laundering and Terrorist Financing Control Regulations – if you have the information, it must be provided.</li> </ul>
24.	<ul style="list-style-type: none"> <li>• Clarification required - Given the similarities in reporting requirements for high-value cash and crypto transactions, we seek clarification on whether the responsibility to collect and report customer data for cryptocurrency transactions exceeding R50,000 rests with the crypto payment service providers or the merchants. Clarifying this responsibility is crucial for aligning our operational processes with FICA requirements and ensuring that all necessary customer data is</li> </ul>	<ul style="list-style-type: none"> <li>• If the entity is an accountable institution (in this case, either item 12 or 22 of Schedule 1 to the FIC Act, that entity has all the FIC Act obligations in respect of their clients. In addition, currently the legislation in respect of CTRs is in respect of fiat transactions, not crypto transactions. However, note the reporting obligations under section 29 of the FIC Act – suspicious transaction reporting.</li> </ul>

**COMMENTS RECEIVED ON DRAFT DIRECTIVE 9 – IMPLEMENTATION OF THE “TRAVEL RULE” RELATING TO CRYPTO ASSET TRANSFERS IN ACCORDANCE WITH THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS**

NO.	COMMENTS RECEIVED	FIC RESPONSE
	accurately recorded and reported in compliance with regulatory expectations.	
25.	<ul style="list-style-type: none"> <li>Para 7 – Commentator proposes that these records be kept for five years from the date of the transaction. This would be in line with standard record retention periods.</li> </ul>	<ul style="list-style-type: none"> <li>The FIC Act specifies the period for which records of clients and transactions must be kept. Records in relation to establishment of a business relationship referred to in section 22 of the FIC Act must be kept for at least five years from the date on which the business relationship is terminated. Records of all transactions concluded referred to in section 22A must be kept for at least five years from the date on which that transaction is concluded. Refer also to GN 7.</li> </ul>
26.	<p><b>Effective date of Directive –</b></p> <p>Most commentators advocated for a transitional period from about 6 months to a year before the Directive enters into force. CASPs will require additional time to deploy their technical solutions fully.</p> <p>If this Directive becomes effective on the date of publication in the Gazette, a crypto asset service provider that fails to comply with a provision of this Directive is non-compliant and is subject to an administrative sanction in accordance with section 45C of the FIC Act.</p>	<ul style="list-style-type: none"> <li>The Travel Rule Directive will enter into force on 30 April 2025.</li> </ul>