March 31, 2023

Securities and Futures Commission
54/F, One Island East
18 Westlands Road, Quarry Bay Hong Kong

Delivered via: VATP-consultation@sfc.hk

Re: Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators licensed by the Securities and Futures Commission

Notabene Inc. welcomes the opportunity to comment on the consultation paper on the "Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators licensed by the Securities and Futures Commission''. We applaud the Securities and Futures Commission for taking the time to put together a comprehensive framework for digital assets and the process undertaken by the Securities and Futures Commission to solicit public engagement on this important topic, and welcome the opportunity to be part of the ongoing dialogue. Notabene has a representation of 32 Hong Kong VASPs entities in our VASP Network[1]. Given the breadth of the topics covered in the request for comment, Notabene will focus primarily on the requirements for virtual asset transfers and requirements in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs.

Introduction and Overview:

Notabene, the crypto industry's only pre-transaction decision making platform, helps to identify and stop high-risk activity before it occurs. The Notabene pre-transaction decision making platform offers a secure, holistic view of crypto transactions, enabling customers to automate real-time decision-making, perform counterparty sanctions screening, identify self-hosted wallets, and complete the smooth roll out of Travel Rule compliance, in line with global regulations.

Notabene was founded in 2020 with the explicit mission to enable safe and trusted crypto transactions by developing a comprehensive solution to help companies comply with the FATF's Travel Rule. A continued strong relationship with global financial regulators including FATF, industry associations, and Virtual Asset Service Providers (VASPs) across multiple jurisdictions arms us with an unparalleled view of the complex and critical nature of regulatory compliance in the crypto space.

[1] https://app.notabene.id/network

Today, many exchanges have AML/CTF processes that allow them to perform customer identification and sanctions screening of their customers as part of onboarding and ongoing customer due diligence. This helps them block sanctioned individuals from directly using their products to initiate transactions. Even with current AML and know your customer (KYC) compliance frameworks in place, VASPs can unknowingly facilitate transactions with sanctioned counterparties.

Only Travel Rule compliance gives VASPs transaction-level counterparty and sanction insight, allowing them to recognize if their clients are sending transactions to sanctioned entities, wallets, or jurisdictions. VASPs worldwide are in different stages of compliance, which leaves many companies vulnerable to exposure to sanctioned individuals.

On page 22 paragraph 64, Securities and Futures Commission states *"Since 2019, the FATF has advocated the importance of applying the wire transfer requirements under FATF Recommendation 16 to virtual asset transfers in a modified form (ie, Travel Rule). The primary objective is to deny illicit actors and designated parties unfettered access to electronically-facilitated virtual asset transfers and detect misuse. The FATF has also reiterated the need for jurisdictions to implement the Travel Rule as soon as possible to address the sunrise issue"*.

Notabene's 2nd annual industry "State Of Travel Rule Report" showed that *Legal uncertainty and the Sunrise Issue remain the leading hindrances to Travel Rule compliance*. On June 7th, 2022, Notabene was the first to introduce a solution that solves the Sunrise issue - we call it SafeTransact-Rise. It enables companies to securely and privately respond to pending Travel Rule data transfers. This plan grants access to our powerful Travel Rule compliance dashboard, allowing Compliance Officers to set up secure automated compliance workflows, and benefit from our award-winning integrations with blockchain analytics and sanctions screening providers. It allows users to perform the mandated VASP due diligence, respond to unlimited Travel Rule data transfers, and send transfers up to 10k USD monthly.

We appreciate the opportunity to respond to this consultation and look forward to continued engagement and clarification.

Very truly yours,

RESPONSE TO CONSULTATION

Below please find our comments and explanations on the various requirements for virtual asset transfers as it pertains in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs.

I. Highlights

In this section, Notabene would like to take the opportunity to highlight the aspects that we find particularly positive about Securities and Futures Commission's proposed approach to regulating crypto Travel Rule in Hong Kong. On a general note, we welcome the fact that the proposed rules on crypto Travel Rule are comprehensive and granular, leaving limited space for regulatory unclarity. In particular, we welcome the clarity provided on the following topics:

1. **Sanction screening obligations**: Section 12.11.2 makes it clear that VASPs need to establish and maintain effective procedures to allow for sanction screening on all relevant parties involved in a transaction, which includes the counterparty end-customer when applicable. Counterparty risk management is the main goal of complying with Travel Rule obligations, but often the

emphasis is on transmitting information rather than how this information should be used to make pre-transaction risk decisions. We welcome the clarity provided in this respect.

2. **Pre-transaction obligations**: In sections 12.11.11 and 12.11.16, the SFC clarifies that Ordering institutions are required to comply with Travel Rule obligations before executing the virtual asset transfer. Notabene welcomes the clarification that Travel Rule compliance needs to be performed pre-transaction. This is particularly important given the specific characteristics of virtual asset transactions: settlement is immediate and irreversible and, hence, only pre-transaction actions can effectively mitigate risk.

3. **Beneficiary information flow**: Section 12.11.20 explicitly requires the beneficiary institution to match the Beneficiary information received from the Originator institution against the information verified by them. This is an essential step in an effective Travel Rule flow that is often not explicitly mentioned in local laws and regulations. Unless the Beneficiary institution complies with this obligation, the Originator institution is assessing counterparty risk (including sanction screening) based on beneficiary information that is self-declared by the originator customer. This section also makes it clear that beneficiary information needs to be transmitted from the Originator to the Beneficiary institution (and the latter is then required to match it against the information that they verified about the beneficiary customer) which helps clarify that implementations of Travel Rule flows where the Beneficiary information is provided by the Beneficiary institution to the Originator institution are not suitable for stopping financial crime and fraud.

II. Comments and requests for clarification

In this section we highlight sections of Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs identified as deserving a comment or a request for clarification.

A. Heightened ML/TF risks of Virtual Assets

Consultation text	**12.10.4** *In relation to the guidance in paragraph 11.3(d) requiring FIs to have policies and procedures for the exceptional situations under which delayed due diligence or evaluation may be allowed, it should be noted that delayed due diligence on the source of a deposit or evaluation of a third-party deposit does not apply to a deposit in the form of virtual assets* ***considering the nature and heightened ML/TF risks associated with virtual assets***.
Notabene's comments	Notabene would like to point out that the nature and heightened ML/TF risks associated with virtual asset illicit activity in cryptocurrency remains a small share of overall volume at less than 1% (0.24% to be exact)[2]. Virtual assets in nature provide the ability to trace potential illicit activity in a way that fiat cannot. Through the Travel Rule regulation, VASPs have the ability to identify and stop illicit transactions before they occur on the blockchain through sanctions screening name and wallet addresses.

B. Risk mitigation on deposits without required Travel Rule information

Consultation text	**12.10.5** *To facilitate the prompt identification of the sources of deposits in the form of virtual assets,* ***FIs are strongly encouraged to whitelist accounts (or wallet addresses as appropriate) owned or controlled by their clients*** *or any acceptable third parties for the making of all such deposits.*

[2] https://go.chainalysis.com/2023-crypto-crime-report.html

	12.11.22 *In respect of the risk-based policies and procedures referred to in paragraph 12.11.21, if an ordering institution or another intermediary institution (hereafter referred to as "instructing institution") from which an instructed institution receives the transfer instruction does not submit all of the required information in connection with the virtual asset transferred to the instructed institution, the instructed institution must as soon as reasonably practicable obtain the missing information from the instructing institution.* ***If the missing information cannot be obtained, the instructed institution*** *should either consider restricting or terminating its business relationship with the instructing institution in relation to virtual asset transfers,* ***or take reasonable measures to mitigate the risk of ML/TF involved.***
Notabene's comments	It would be beneficial to provide additional guidance on what is deemed a reasonable measure to mitigate the ML/TF risks when relevant Travel Rule information cannot be obtained from the Instructing institution, under 12.11.22. Section 12.10.5 encourages VASPs to whitelist accounts to facilitate the prompt identification of the source of the deposit. It would be helpful to clarify whether this process constitutes a reasonable measure for the purposes of Section 12.11.22. Additionally, VASPs should be permitted to implement measures to identify the source of the deposit both pre-transaction (often referred to as a whitelisting process) and at the point of transaction, before the funds are made available to the beneficiary end-customer. Notabene would advise and encourage to be less tech prescriptive for this section due to rapid dynamic phases of crypto and crypto fraud where whitelisting processes may not catch or update in time. Instead, we would encourage dynamic measures to deal with real time risk.

C. Wallet ownership verification in VASP to VASP transactions

Consultation text	**12.10.6** *For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, the required originator or recipient information verified by the ordering or beneficiary institution may be sufficient for an FI to ascertain whether the transaction involves a third party 127. Conversely,* ***where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should ascertain the customer's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the unhosted wallet, by taking appropriate measures****, for example:* *a. using appropriate confirmation methods 128 [128 Examples of confirmation methods may include requesting the customer to perform the micropayment test (i.e. by effecting a virtual asset transfer with an (typically small) amount specified by the FI) or message signing test (i.e. by signing a message specified by the FI which is then verified by the FI).]; and* *b. obtaining evidence from the customer such as a statement of account issued by the VA transfer counterparty.*
Notabene's comments	The guidance provided with respect to transacting with higher ML/TF risks VASPs and unhosted wallets only addresses first-party transactions. VASPs are required to assess their own customer's ownership or control over the account with the higher ML/TF risks VASP or unhosted wallet. It would be beneficial to clarify the expectations for third-party transactions. For example, if the unhosted wallet or account with the higher ML/TF risks VASP is owned or controlled by a third-party, what obligations would apply? This is particularly relevant because the measures suggested to establish control are more challenging to apply when facilitating a transaction with a third-party that does not have a relationship with the VASP. Additionally, if the intention of these provisions is to

	prohibit third-party transactions with self-hosted wallets, Notabene would comment that this would be an ineffective and disproportionate restriction. If prohibited to facilitate transactions with unhosted wallets of third-parties, the VASP's customer can still transfer funds to their own wallet and subsequently to the third party wallet (and vice-versa for deposits). This will create a blindspot that backfires on the regulatory goals: the VASP will have less visibility on the transactions between their customers and unhosted wallets controlled by third-parties. Further, as mentioned below (II. O (Unhosted Wallets)) transactions with unhosted wallets shall not be deemed inherently high risk. This provision also requires VASPs to apply ownership or control verification measures when transacting with other VASPs. This requirement is excessively burdensome. In VASP to VASP transactions, the identification of account owners should be assessed via compliant Travel Rule flows that allow VASPs to exchange identifying information about the originator and beneficiary customers.

D. Travel rule in the context of internal transactions

Consultation text	**12.11.4** *Section 13A of Schedule 2, paragraphs 12.11.5 to 12.11.23, 12.12 and 12.13 apply to a virtual asset transfer that is a transaction carried out:* *a. by an institution (the ordering institution) on behalf of a person (the originator) by transferring any virtual assets; and* *b. with a view to making the virtual assets available:* *i. to that person or another person (the recipient); and* ***ii. <u>at an institution (the beneficiary institution), which may be the ordering institution or another institution,</u>***

Notabene's comments	Under section 12.11.4 Travel Rule obligations apply to transactions carried out with a view to making virtual assets available at an institution which may be the Ordering institution or another institution. This seems to include intra-VASP transfers within the scope of the Travel Rule. On this aspect, Notabene would welcome further clarification on whether, in these cases, the verification of the originator and the beneficiary information by the VASP, as part of its customer due diligence obligations, suffices, and no information transmission is required. Notabene takes the view that this interpretation would be sensible as we fail to see the utility of transmitting information within the VASP. It may be beneficial to state the intention of the provision more explicitly.

E. Scope of required Travel Rule information

Consultation text	**12.11.5** *Before carrying out a virtual asset transfer involving virtual assets that amount to not less than $8,000, an ordering institution must obtain and record the following originator and recipient information131:* *a. the originator's name;* *b. the number of the originator's account maintained with the ordering institution and from which the virtual assets are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the ordering institution;* ***c. the originator's address 132 , the originator's customer identification number 133 or identification document number or, if the originator is an individual, the originator's date and place of birth;*** *d. the recipient's name; and* *e. the number of the recipient's account maintained with the beneficiary institution and to which the virtual assets are transferred (i.e. the account used*

	to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the beneficiary institution.
Notabene's comments	Notabene would welcome clarification on whether all data points mentioned in point c) above are alternatives between each other, since there is no "or" in between originator address and originator customer identification number. The wording would be more clear if structured as follows: *Before carrying out a virtual asset transfer involving virtual assets that amount to not less than $8,000, an ordering institution must obtain and record the following originator and recipient information131:* *f. the originator's name;* *g. the number of the originator's account maintained with the ordering institution and from which the virtual assets are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the ordering institution;* *h. On of the following:* ***i. <u>the originator's address; or</u>*** ***ii. <u>the originator's customer identification number; or</u>*** ***iii. <u>identification document number; or</u>*** ***iv. <u>if the originator is an individual, the originator's date and place of birth;</u>*** *i. the recipient's name; and* *j. the number of the recipient's account maintained with the beneficiary institution and to which the virtual assets are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the beneficiary institution.*

F. Travel Rule as a pre-transaction requirement

Consultation text	**12.11.11** *"Immediately" referred to in paragraph 12.11.9 means that the ordering institution should submit the required information* ***prior to, or simultaneously or concurrently with, the virtual asset transfer*** *(i.e. the submission must occur before or when the virtual asset transfer is conducted)134.* **12.11.16** *The ordering institution* ***should not execute a virtual asset transfer unless it has ensured compliance*** *with the requirements in paragraphs 12.11.5 to 12.11.15.*
Notabene's comments	Notabene welcomes the clarification that ordering institutions are required to comply with the requirements in 12.11.5 to 12.11.15 before transacting. On this matter, we would like to point out that, ideally, the obligations of the Beneficiary institution mentioned in 12.11.20 [confirming "*whether the recipient's name and account number obtained from the institution from which it receives the transfer instruction match with the recipient information verified by it*"] should also ideally be fulfilled before the transaction is initiated. This aspect highlights one of the key differences between crypto and traditional payments. In a traditional SWIFT payment, settlement might happen a couple times during the day, which gives time for the beneficiary to send a message back requesting that the funds are withheld (e.g., due to a beneficiary name mismatch). In crypto transactions, settlement is immediate and irreversible. Hence, to effectively fulfill the goals of the Travel Rule, the beneficiary VASP should react to the information transmission before the transaction is sent. Otherwise, VASPs are unable to effectively carry out duties such as beneficiary name matching and sanctions screening prior to receiving the funds and, depending on their system, prior to the funds being released to the end-customer.

	However, VASPs should be able to take a risk based approach to deciding whether or not to wait for a response from the Beneficiary VASP before executing the transaction, to unburden VASPs and facilitate transaction flows in low risk scenarios and during the sunrise period (where responses from Beneficiary VASPs may take longer or never arrive).

G. Data protection arrangements

Consultation text	**12.11.12** *To ensure that the required information is submitted in a secure manner, an ordering institution should136:* *a. (...)* *b. take other appropriate measures and controls, for example:* *i. entering a bilateral data sharing agreement with the beneficiary institution and, where applicable, the intermediary institution* ***and/or*** *(where applicable)* ***a service-level agreement with the technological solution provider for travel rule compliance*** *(see paragraphs 12.12) which specifies the responsibilities of the institutions involved* ***and/or*** *the provider to ensure the protection of the confidentiality and integrity of the information submitted;*
Notabene's comments	Notabene welcomes that this topic is covered as it is a source of legal operational hurdles for VASPs rolling out Travel Rule compliance. We would welcome clarification on whether the existence of a data processing agreement between each VASP and the technology provider suffices. E.g., if VASP A and VASP B both have a data processing agreement with the technology provider, is this enough to be able to transmit information between each other using said technology provider, even in the absence of a bilateral agreement? This would be beneficial, as it is operationally challenging and cost-intensive to enter into bilateral agreements with each counterparty VASP.

H. Conciliation between data privacy and Travel Rule

Consultation text	**12.11.12** *For the avoidance of doubt, an ordering institution* ***should not execute a virtual asset transfer when it could not ensure that the required information could be submitted to a beneficiary institution****, and where applicable, an intermediary institution, in a secure manner having regard to the above guidance and the VA transfer counterparty due diligence results.*
Notabene's comments	Notabene would like to point out that this approach is stricter than the one suggested by the FATF guidelines in this respect. In paragraph 291 of the Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, the FATF recommends that: "*VASPs should have recourse to altered procedures, including the* ***possibility of not sending user information, when they reasonably believe a counterparty VASP will not handle it securely while continuing to execute the transfer if they believe the AML/CFT risks are acceptable****. In these circumstances, VASPs should identify an alternative procedure, whose control design could be duly reviewed by their supervisors when requested.*" Notabene supports the approach taken by the FATF as a reasonable means to handle the conflict between AML/CTF goals and data protection. In scenarios where the risk of money laundering and terrorism financing is low, but data privacy risks are high, it is reasonable to allow VASPs to transact without sharing Travel Rule information. For this exception to be effective and to avoid that it creates an unintentional loophole in Travel Rule compliance, we identify two measures that would be required: 1. The criteria that VASPs should use to determine that their counterparty does not have adequate safeguards for ensuring data protection needs to be specified and VASPs should be required to document their reasoning; 2. In line with recommendations in paragraph 291 of the FATF Guidance, VASPs should be required to apply alternative procedures - duly reviewed and

	controlled by the supervisory authorities - to achieve the goals of the Travel Rule to the extent possible. Requiring the Originator VASP to collect and share beneficiary information could be seen as a minimum requirement, considering that the Beneficiary VASP already should know this information and it would be required to match a beneficiary with the underlying account.

I. Intermediary institutions obligations with regards to self-hosted wallets

Consultation text	**12.11.17** *An intermediary institution must ensure that **all originator and recipient information as set out in paragraphs 12.11.5 and 12.11.6** which the intermediary institution receives in connection with the virtual asset transfer is retained with the required information submission, and is transmitted to the institution to which it passes on the transfer instruction141.*
Notabene's comments	Notabene would welcome clarification on what requirements apply when an Intermediary institution is involved in facilitating a transaction to/from an unhosted wallet. In particular, it would be relevant to clarify whether the Intermediary institution is required to receive: a. The information mentioned in section 12.14.2, and b. The results on the ownership/control verification mentioned in sections 12.10.6 and 12.10.7.

J. Beneficiary name matching and beneficiary information flow

Consultation text	**12.11.20** *The beneficiary institution should also confirm whether the recipient's name and account number obtained from the institution from which it receives the transfer instruction match with the recipient information verified by it, and take reasonable measures as set out in paragraph 12.11.23 where such information does not*

	match.
Notabene's comments	We would recommend that the result of this assessment (i.e., the received information matches the verified recipient information *or* the received information does not match the verified recipient information) is shared with the Originator VASP. Unless the Beneficiary institution complies with this obligation and shares the result with the Originator institution, the latter is assessing counterparty risk (including sanction screening) based on beneficiary information that is self-declared by the originator customer. If any mismatch is detected, it is important that the Originator VASP is aware of it. On this topic, please also refer to our comments on **II.F** above (Travel Rule is a pre-transaction requirement).

K. Incomplete Travel Rule information in cross-border transactions

Consultation text	**12.11.23** *If the instructed institution is aware that any of the information submitted to it that purports to be the required information is **incomplete** or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved having regard to the procedures set out in paragraph 12.11.21(b).*
Notabene's comments	When the Originator institution operates outside Hong Kong, they may be subject to a different scope of information transmission requirements. For instance, several jurisdictions do not require VASPs to transmit information for transactions below a certain threshold. Others, require VASPs to submit a more limited scope of information than that required under sections 12.11.5 and 12.11.6. Notabene would welcome a reference to this particularity of transacting cross-borders as an aspect that VASPs should consider when deciding on the procedures set out in paragraph 12.11.21(b) - if the Originator VASP complied with Travel Rule obligations as they apply in their jurisdiction, VASPs should be able to accept the funds unless there is a high ML/TF risk that needs to be accounted for.

L. Counterparty VASP due diligence as an obligation of the VASP

Consultation text	**12.12.2** *Where an FI chooses to use a technological solution for ensuring travel rule compliance (hereafter referred to as "solution"), the FI* ***remains responsible for discharging its AML/CFT obligations*** *in relation to travel rule compliance.* **12.12.3** In addition, an FI should consider a range of factors as part of the due diligence on the solution, such as: a. (...) b. (...) c. (...) **d.** *whether the* ***solution facilitates the FI in conducting VA transfer counterparty due diligence*** *(see paragraphs 12.13) and requesting for additional information from the VA transfer counterparty as and when necessary.*
Notabene's comments	From the two provisions cited above, it seems clear that VASPs are responsible for carrying out due diligence on their counterparties and cannot rely on the assessment of technology providers for those purposes. This is an area that is not always fully understood by the industry - there is still confusion on whether VASPs should be able to rely on the due diligence performed by the technology provider to discharge their obligation. Hence, Notabene would recommend that section 12.12.2 makes a specific reference to the counterparty due diligence obligations: although the technology solution can and should facilitate the counterparty due diligence process, the FI remains **responsible** for making its own assessment and cannot rely on the due diligence conducted by the technology solution.

M. Interoperability vs Reachability

Consultation text	**12.12.3** *In addition, an FI should consider a range of factors as part of the due diligence on the solution, such as:*

	*a. the **interoperability** of the solution **with other similar solution(s) adopted by the VA transfer counterparties that the FI may deal with**;*
Notabene's comments	Rather than focusing on the interoperability between solutions, Notabene recommends that FIs assess which counterparties they are able to reach through the solution and hence focus on reachability. As is further explained below, interoperability is currently very limited due to the existence of closed networks.. Hence, VASPs should focus on the coverage enabled by each technology provider. Some of the existing technology providers are structured as closed Travel Rule protocols. In this model, a central entity decides which VASPs are able to send and receive Travel Rule data transfers through the protocol. Currently, VASPs need to solve two hurdles to be able to reach counterparties that are members of closed-network protocols: 1. Join those networks as a member; and 2. Integrate one or more protocols directly or integrate with an interoperable protocol / solution. A comprehensive solution to the first hurdle (join closed-networks as a member) without regulatory intervention is difficult to envision because membership of closed network protocols is not available to all VASPs and is dependent on discretionary approval from the entities running the closed-network. This, considering that these closed networks are run by VASPs with significant market share, poses antitrust concerns that can only be addressed at a regulatory level. On the second hindrance (integration with the protocol): once a VASP becomes a member of the closed network, they are free to technically integrate. However, managing several integrations to be able to exchange Travel Rule information with different silos of VASPs is cumbersome and prevents an effective implementation of Travel Rule

	compliance. The solution for this would be to integrate with solutions that are protocol agnostic and can manage the switch between the protocols in each transaction. There are already multiple technical solutions to plug all protocols to a protocol-agnostic solution and achieve interoperability. However, these solutions are challenging to implement without the cooperation of these closed networks, which, in turn, do not have a commercial incentive to enable interoperability.

N. Counterparty VASP due diligence measures

Consultation text	**12.13** *VA transfer counterparty due diligence and additional measures*
Notabene's comments	Notabene would like to make a few general comments on counterparty due diligence obligations for Travel Rule purposes. 1. We welcome that, in line with the FATF guidelines, the SFC recognizes that counterparty due diligence for the purposes of engaging in Travel Rule flows is distinct from the due diligence required to establish correspondent banking relationships. The nature of VASPs relationships' for transacting with one another and sharing Travel Rule information is very distinct from correspondent banking relationships. Hence, we agree with the FATF and SFC stance that the required due diligence obligations should also be different, and more limited in scope. 2. Counterparty due diligence for Travel Rule purposes is a burdensome requirement for VASPs as it entails carrying out an assessment of each counterparty VASP they transact with. Therefore, we believe it is important to establish a framework that allows for simplified due diligence when appropriate, to

	ensure that this is a component of Travel Rule compliance that VASPs can realistically implement. 3. Below, we list proposed simplifications: a. Hong Kong VASPs should be able to transact and share Travel Rule information with other regulated VASPs within the country, relying on the uniform requirements and supervision applied. No due diligence requirements should apply in these cases. This could also apply to any jurisdictions that Hong Kong deems as enforcing equivalent VASP supervision and data protection rules; b. For transacting and sharing Travel Rule information outside Hong Kong (or equivalent jurisdictions), VASPs should be required to apply a simplified due diligence process that focuses on: (i) complete identification of the counterparty VASP - Chapter 12 could offer guidance as to what is considered reliable data sources for identification of the counterparty VASP; and (ii) assess whether the counterparty VASP is an eligible counterparty to send customer data to and to have a business relationship with, based on factors such as: i. the robustness of the data privacy and security obligations enforced in the counterparty's jurisdiction; and ii. the licensing and registration requirements of the jurisdiction where the VASP is based (FATF evaluations can be taken into account). c. Enhanced due diligence measures can be required for transacting and sharing Travel Rule information with VASPs based in high-risk jurisdictions.

Consultation text	*An FI should apply the following VA transfer counterparty due diligence measures before it conducts a virtual asset*

	transfer with a VA transfer counterparty: *a. (...);* ***b. <u>understand the nature and expected volume and value of virtual asset transfers with the VA transfer counterparty</u>;***
Notabene's comments	Notabene would welcome clarification on how this can be assessed before conducting transfers. Our suggestion would be to clarify that for this assessment VASPs can rely on historical data on transaction volumes with each counterparty.

Consultation text	*An FI should apply the following VA transfer counterparty due diligence measures before it conducts a virtual asset transfer with a VA transfer counterparty:* *a. (...)* *b. (...)* *c. determine from publicly available information the reputation of the VA transfer counterparty and the quality and effectiveness of the AML/CFT regulation and supervision over the VA transfer counterparty by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs*
Notabene's comments	We would welcome an explicit acknowledgement that VASPs are able to rely on the assessments on countries' AML/CTF regulation and supervision carried out by international bodies - e.g., the evaluations carried out by the FATF.

O. Unhosted wallets

Consultation text	**12.14.1** *An* **<u>FI should exercise extra care *in respect of the risks posed by virtual asset transfers to or from unhosted wallets</u>*** *153 and peer-to-peer transactions associated with unhosted wallets, which may be attractive to illicit actors given the anonymity, mobility and usability of virtual assets and that there is typically no intermediary involved in the peer-to- peer transactions to carry out AML/CFT*

	measures such as CDD and transaction monitoring.
Notabene's comments	Notabene takes the view that transacting with unhosted wallets shall not be deemed as inherently higher risk and requiring extra care. For instance, in cases where the VASP is able to verify that the unhosted wallet is controlled by their own customer, this could reflect a lower risk considering that the VASP facilitates a transaction with a known and risk-monitored customer. Unhosted wallets play a key role in the cryptocurrency ecosystem and they are often used for legitimate use cases – individuals as well as exchanges use them to securely move funds and hold long term investments. Blockchain analysis tools can provide VASPs with the appropriate data regarding unhosted wallets to conduct their risk assessment, mitigate risks and back their decision in front of the regulators. The data shows that the majority of the funds held in unhosted wallets often come from VASPs and are related to investing purposes or are the vehicle for individuals or organizations to move funds between regulated exchanges. [3]

[3] https://blog.chainalysis.com/reports/travel-rule-compliance-unhosted-wallets/