Response to EBA Consultation Paper EBA/CP/2023/42

Two sets of Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures

2. Guidelines on internal policies, procedures and controls to ensure the implementation of EU and national restrictive measures under Regulation 2023/1113/EU

4.1.2 List management – point 8, 9, 10, 11, 12 & 13

""8. PSPs and CASPs should specify in their policies and procedures the national, supranational and international restrictive measures regimes to which they are subject.
9. PSPs and CASPs should have policies and procedures to:
a. identify when a new set of restrictive measures is adopted, or an existing restrictive measure is updated or lifted;
b. update their internal data set to be screened in compliance with Section 4.1.3 when a new restrictive measure is adopted, or an existing restrictive measure is updated or lifted."

VBNL wants to emphasize that CASPs already do have such measures in place, and CASPs use service providers for the screening on restrictive measures. Despite our view that CASPs itself remains responsible for the screening process, VBNL would like to stress that CASPs are also partly dependent on their vendors. As CASPs cannot influence the vendor to add information or remove information, it asks assurances from the vendor that they update the lists. CASPs have no alternative but to consider the option of switching vendors if the current one fails to fulfill its contractual obligations, which often includes periodic checking of a list. In addition, VBNL wishes to highlight that vendors rely on the consolidated lists published by the European Commission (EC) to monitor new sanctions. Despite CASPs being required to promptly implement these changes, the main challenge observed by CASPs lies in obtaining timely updates from the EC. Specifically, there appears to be a gap of approximately three working days between the implementation of legal changes and the updating of the consolidated list.

"10. PSPs and CASPs should define in their policies and procedures the types of data they will screen for each type of restrictive measure, taking into account the outcome of their restrictive measures exposure assessment and the restrictive measures they have to apply.
11. When deciding the set of data to be screened according to the type of applicable restrictive measure, PSPs and CASPs should consider all data they hold about their customers, including information obtained:
a. when applying customer due diligence measures in line with Directive (EU) 2015/849 as transposed by national law; and
b. when complying with Regulation (EU) 2023/1113.
12. PSPs and CASPs should assess whether the data they hold is sufficiently accurate, up to date and detailed to enable them to establish if a party to the transfer or their beneficial owner or proxy is subject to restrictive measures pursuant to Regulation (EU) 2023/1113.

Regarding paragraph 11(b) and 12, the VBNL wishes to emphasize that while CASPs can screen the received data, the effectiveness of such screening is uncertain if the data itself is inaccurate. VBNL highlights that the data held by CASPs is typically more comprehensive and accurate compared to the information found on sanctions lists, which often contain incomplete and inaccurate data. Specifically, VBNL notes that the EU and United Nations (UN) lists lack a thorough and precise collection of elements.

4.1.5 Screening of transfer of funds and crypto-assets – point 20, 21, 22 and 23

'20. PSPs and CASPs should screen all transfers of funds and crypto-assets prior to their completion, whether they are carried out as part of a business relationship or as part of a one-off transaction.'

VBNL wishes to highlight that in principle, due to the immutability of the blockchain network, it is technically impossible to screen incoming crypto-asset transfers prior to their execution. While there are technical capabilities to screen the mempool (the queue of transactions yet to be executed on the bitcoin blockchain), this entails numerous complexities and often does not provide certainty. The best effort in the sector will therefore likely result in segregation of assets until information is received to screen all parties. During the initial phase of implementation, we expect there are various instances when CASPs are unable to comply with the screening of incoming transfers from counterparty CASPs, due to the insufficiency or complete lack of information they might send. We ask that the ESAs acknowledge this initial unlevel playing field.

'21. PSPs and CASPs should screen all parties to transfers of funds or crypto-assets against the restrictive measures-related lists. Intermediary PSPs and CASPs should pay special attention in their restrictive measures exposure assessment to the soundness and reliability of the restrictive measures policies and procedures put in place by PSPs and CASPs they are doing business with to ensure compliance with restrictive measures.'

Many crypto-asset transfers are made in which the originator and beneficiary are the same person. VBNL is of the opinion that it should be clear that the transfer should not in each case be the incentive to screen. Rather the incentive should be that when new parties are involved in the transfer that those are screened against restrictive measures-related lists. If screening is required to take place at every transfer regardless this would cause CASPs to make costs for checking against restrictive measures-related lists and can hamper the flow of transfers if screening is required whenever a transfer is initiated.

'22.Details to be screened should include at least:

a) *identifying data of the payer/originator and the payee/beneficiary stipulated in Articles 4 and 14 of Regulation (EU) 2023/1113;*
b) *the purpose of the transfer of funds or crypto-assets and other free text fields that provide further information regarding the actual sender/recipient of funds or crypto-assets;'*

VBNL wishes to emphasise that in order to comply with 22(a), so without collecting the date of birth, the screening will rely solely on names, potentially leading to numerous false matches. In addition, with regard to 22(b), only in limited cases there will be text fields that provide further information to screen. Only for transfers from CASP to CASP there is the option through a vendor solution to send a message in the form of a text field. Guidance around how free text fields can be used to ensure compliance with restrictive measures would give clarity around these expectations.

'23. Where data identifying the payee of a transfer of funds or beneficiary of a transfer of crypto-assets is missing or meaningless, the PSPs and CASPs should, in line with the provisions in Section 6.1 of the Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 ('The Travel Rule Guidelines'), decide whether to execute, reject or suspend the transfer. Any new information obtained subsequently, before or after executing the transfer, should also be screened.'

It's currently unclear whether CASPs will receive correspondence from the payment service provider (PSP) during transactions between CASPs. If the PSP doesn't transmit this information, CASPs won't receive it, relying solely on beneficiary details they already have. Despite this, CASPs can't decline the transfer even if they choose to for reasons like blockchain analysis or internal risk assessment. Any

refusal would still lead to a refund or a new outgoing payment from the CASPs' crypto address, making it technologically impossible for CASPs to reject such transfers. Guidance on situations where CASPs suspend the payment, and what CASPs should do while waiting for local authorities to decide what CASPs should do while waiting for the FIU to decide what to do with the frozen funds.

4.2.2 Due diligence measures for alert analysis - point 34

'In case of doubt about the trueness of a match, PSPs and CASPs should use additional information they may hold to support the analysis of alerts to the extent that this information is available'

In practice the beneficiary CASP receives limited information from the counterparty CASP. Specifically the date of birth is not required information to share before executing the transfer. Lacking data points such as date of birth will cause the CASP to handle many false positives. Considering that screenings against restrictive-measures lists are performed before executing the transfer it is important that we are aware in the sector that this can cause a significant constraint on CASPs to quickly assess true / false positives and can slow down the speed at which transfers are made if calibration is not done accurately.

4.2.4 Controls and due diligence measures to comply with sectoral restrictive measures – point 40

'PSPs and CASPs should pay particular attention to sectoral restrictive measures that are related to a specific jurisdiction or territory. Under such restrictive measures, PSPs and CASPs should screen all underlying information relating to the transfer of funds or crypto-assets to or from that specific jurisdiction or territory or to transfers of funds or crypto-assets initiated by customers who are known to conduct business in that specific jurisdiction or territory. To the extent that this is available, PSPs and CASPs should screen:
a. information on the country (ies) of nationality, place of birth;
b. information on the habitual residence or place of activity through other addresses;
c. information on the country to or from which the transfer of funds or crypto-assets is carried out, where the transfer of funds or crypto-assets is executed;
d. purpose of the transfer of funds or crypto-assets and other free text fields that provide further information regarding the goods, vessels, country of destination or country of origin of the goods for which the payment is made.'

It is important to be aware that crypto-asset transfers by default have an international nature and are borderless. CASPs that pay attention to sectoral restrictive measures will be able to do so on their own customer population based on available data. It will be more difficult to assess for restrictive measures with regards to the counterparty in the crypto asset transfers.

Point c mentions *'information on the country to or from which the transfer of funds is carried out, where the transfer of funds or crypto-assets is executed'*. Guidance on leading and supportive indicators would help for future assessements. It is for example unclear how the address of the originator should be used to make this assessment or if there are other indicators leading such as the country of incorporation of the sending CASP. In addition, it should be noted that it is not possible to ascertain with certainty the country from which a crypto-asset transfer is initiated or executed. Therefore, it may be preferable to exclude crypto-assets in this context.