THE LATEST FATF GUIDANCE FOR VASPS

SOME KEY POINTS

Andrea Berruto - FinTech Lawyer
at
"Karuna Ethical Blockchain Advisory"

KARUNA
ETHICAL BLOCKCHAIN ADVISORY

FATF HAS JUST A FOCUS ON RISKS

VAs have certain potential ML/TF risks, including their global reach, capacity for rapid settlement, ability to enable P2P transactions, and potential for increased anonymity and obfuscation of transaction flows and counterparties.

OBTAINING AND HOLDING REQUIRED AND ACCURATE ORIGINATOR AND BENEFICIARY INFORMATION

The *ordering* institution must *obtain* and *hold* the following information:

- originator's accurate full name ("accurate" means "verified");
- originator's accurate account number (e.g., the "wallet address" of the VA) where such an account is used to process the transaction;
- originator's accurate address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;
- beneficiary's full name (i.e., the name of the person who is identified by the originator as the receiver of the VA transfer). This is not required to be verified by the ordering institution for accuracy, but should be reviewed for the purpose of STR monitoring and sanction screening; and
- beneficiary account number, where such an account is used to process the transaction.

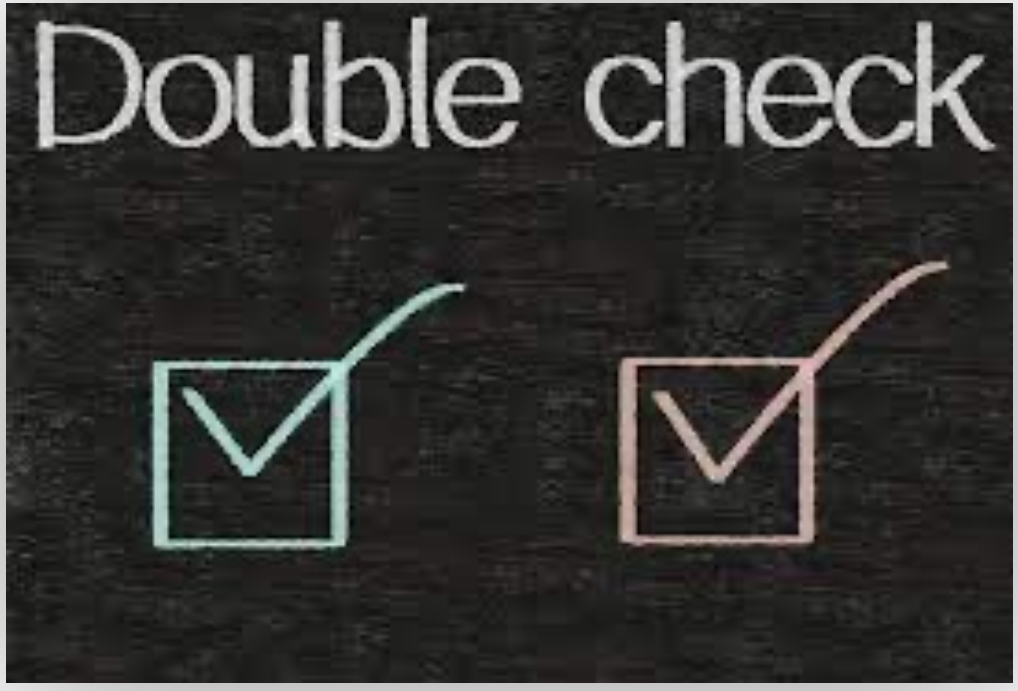
OBTAINING AND HOLDING REQUIRED AND ACCURATE ORIGINATOR AND BENEFICIARY INFORMATION

On the other hand, the *beneficiary* institution must *obtain* from the originator institution and *hold,* the below information:

- originator's full name, which does not have been verified by the beneficiary institution for accuracy (it must however be reviewed for the purpose of STR monitoring and sanction screening);
- originator's account number, where such an account is used to process the transaction;
- originator's address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;
- beneficiary's full name, which must be verified for accuracy, if not already previously verified; and
- beneficiary's account number.

SCREENING FOR VA TRANSFERS

The ordering and beneficiary institutions must then screen the names of the other party (the originator or the beneficiary) when they conduct the VA transfer.



IMMEDIATE AND SECURE SUBMISSION OF INFORMATION

The ordering institution must *submit* the required information to the beneficiary institution (if any) *immediately* and *securely*.

"Immediately" means that the required information must be submitted prior, simultaneously or concurrently with the transfer itself. *Post facto* submission of the required information should not be permitted.

"Securely" means that the required information must be transmitted and stored in a secure manner, so as to protect the integrity and availability of the required information to facilitate record-keeping, facilitate the use of such information by receiving VASPs or other obliged entities and protect the information from unauthorized disclosure.

IMMEDIATE AND SECURE SUBMISSION OF INFORMATION

Submitting information to the beneficiary VASP could be an entirely distinct process from that of the blockchain or other DLT VA transfers.

Any technology or software solution is acceptable, provided that the solution enables the ordering and beneficiary institutions to comply with the above requirements.

TRANSFERS BELOW 1,000 EUR

If a country decides to adopt a *de minimis* threshold for VA transfers of EUR 1,000, and. For VA transfers under the threshold, fewer requirements apply to VASPs, that may simply collect:

- ❑ originator's name
- ❑ beneficiary's name; and
- ❑ the VA wallet address for each or a unique transaction reference number.

Such information does not need to be verified unless there are ML/FT suspicious circumstances.

VA TRANSFERS TO/FROM OTHER VASPS AND COUNTERPARTY VASP IDENTIFICATION AND DUE DILIGENCE

For a VASP to transmit the required information to another VASP, it is necessary to identify and conduct due diligence on their counterparty VASP before transmitting the required information. VASPs do not need to undertake the counterparty VASP due diligence process for every individual VA transfer when dealing with VASPs for which they have previously conducted counterparty due diligence, unless there is a suspicious transaction history or other information (such as adverse media, published information about regulatory or criminal penalties) indicating they should. 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.

VA TRANSFERS TO/FROM UNHOSTED WALLETS

"The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer (e.g., when an ordering VASP or other obliged entity sends VAs for or on behalf the originator to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer to an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be)."

VA TRANSFERS TO/FROM UNHOSTED WALLETS

"The FATF does not expect that VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities. VASPs sending or receiving a VA transfer to/from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user to an unhosted wallet), should obtain the required originator and beneficiary information from their customer. Countries should require their VASPs or other obliged entities to implement mechanisms to ensure effective scrutiny of such transfers, in particular to meet their STR and sanctions implementation obligations (see the discussion of Recommendation 20 below) and, as discussed above, may choose to impose additional limitations or controls on such transfers with unhosted wallets."

VA TRANSFERS TO/FROM UNHOSTED WALLETS

FATF requires VASPs to collect data on their unhosted wallet transfers (via their customers) and to monitor and assess that information as necessary to determine to what extent a transaction is within their risk appetite, and the appropriate risk-based controls to apply to such a transaction/individual customer. Key ML/FT indicators include:

- Technological features that increase anonymity;
- Geographical risks;
- Transaction patterns;
- Transaction size;
- Sender or recipient profiles; and
- Source of funds or wealth.

However, FATF does not require VASPs to "submit" the required information to individuals who are not obliged entities; FATF simply requires that VASPs effectively scrutinize such transfers, in particular, to meet their STR and sanctions implementation obligations.