

Frequently Asked Questions (FAQs) on the Guidelines for Virtual Asset Service Providers (Circular No. 1108 dated 26 January 2021)

Why are Virtual Currencies (VC) and VC Exchanges (VCE) now referred to as Virtual Assets (VA) and Virtual Asset Service Providers (VASP)?

The BSP has decided to refer to **virtual currencies** as defined under Circular No. 944 dated 06 February 2017 as “**virtual assets**” or **VAs**, in recognition of the evolving nature of this financial innovation. We have adopted the definition espoused by the Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog, in referring to cryptocurrencies and other digital assets harnessing such technology.

In the same manner, the virtual asset market has developed business models beyond the exchange and conversion between virtual currencies and fiat currencies. Adopting the FATF’s definition of “**virtual asset service providers**” better captures such developments.

Overall, this provides the BSP’s regulatory framework with the flexibility to handle a fast-moving and technologically dynamic sector.

How do VCs differ from VAs?

VAs refer to any type of digital unit that is used as a medium of exchange or form of digitally stored value created by agreement within the community of VC users. VA expands on the definition of VC by highlighting the use of such digital unit beyond the typical functions of a currency (i.e., VAs refer to any type of digital unit that can be digitally traded, or transferred, and can be used for payment or investment purposes). Similar to VCs, VAs are not issued nor guaranteed by any jurisdictions and do not have legal tender status.

For the purposes of applying the FATF Recommendations on anti-money laundering, the BSP also considers all funds- or value-based terms in the FATF Recommendations, such as “property,” “proceeds,” “funds,” “funds or other assets,” and other “corresponding value,” to also include and be applicable to VAs.

Digital units of exchange that is used for (i) the payment of goods and services solely provided by its issuer or a limited set of merchants specified by its issuer (e.g., gift checks); or (ii) the payment of virtual goods and services within an online game (e.g., gaming tokens) are also not considered as VAs in the context of the BSP’s guidelines.

How do VCEs differ from VASPs?

VCEs as defined in BSP Circular No. 944 dated 06 February 2017 only covers businesses involved in the exchange of fiat currency and virtual currency. BSP Circular No. 1108 expands the scope of activities to be regulated as VASPs to include businesses that perform

- exchange between one or more forms of VAs;
- transfer of VAs; and
- safekeeping and/or administration of VAs or instruments enabling control over VAs.

This is to ensure that activities relating to VASP are executed within an unbroken chain of regulated entities.

What are VA Custodians (i.e., VASP with safekeeping and/or administration of VAs)?

Follow the FATF Guidance on VAs and VASPs¹, the BSP recognizes VA custodians as entities that provide services or business models that either (i) safeguards the customer's VA wallet; and/or (ii) permits the VASP to manage the customer's VA wallet.

As an example, a VASP with capabilities to execute VA transfers on behalf of the customer through its platform can be considered as a VA Custodian. They may also have the ability to create and secure VA wallets of their customers through their platform. In addition, the FATF Guidance considers safekeeping and administration services to include businesses that "have exclusive or independent control of the private key associated with VAs belonging to another person or exclusive and independent control of smart contracts to which they are not a party that involve VAs belonging to another person."

The BSP shall use such basis as well as documentations from the applicant in evaluating whether a VASP provides VA custodial services or not.

What is the "travel rule" requirement and how does it apply to VASPs?

The VASP guidelines emphasizes that all transactions involving the transfer of VA shall be treated as cross-border wire transfer and that VASPs are expected to comply with corresponding BSP rules governing wire transfer, particularly on the obligation to provide immediate and secure transmittal of originator and beneficiary information from one VASP to another for certain transactions. This particular requirement is also commonly known as the "travel rule" across jurisdictions.

The travel rule aids in the prevention of money laundering and other financial crimes by maintaining an information trail about individuals that send and receive funds.

VASPs and other supervised entities must be able to obtain and hold originator and beneficiary information for VA transfers amounting to P50,000.00 or more (or its equivalent in foreign currency) and transmit such information to the receiving institution.

¹ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>

The required information includes the following:

- a. originator's name (*i.e.*, the sending customer);
- b. originator's account number used to process the transaction (*e.g.*, the VA wallet);
- c. any of the following: originator's physical (geographical) address, national identity number, customer identification number that uniquely identifies the originator to the ordering institution, or date and place of birth;
- d. beneficiary's name; and
- e. beneficiary account number where such an account is used to process the transaction (*e.g.*, the VA wallet).

The BSP does not prescribe a specific technology for the obtaining and sending of originator information as well as the obtaining and holding of beneficiary information between VASPs.

VASPs and other obliged entities in VA transfers may leverage on existing commercially viable technology or harness new technologies (*e.g.*, tokenization) to comply with this requirement.

Are VASPs different from Electronic Money Issuers (EMI-Others)?

Below is a table providing a general comparison between two distinct money service business operations: EMI-Others and VASPs².

	Electronic Money Issuer (EMI-Others)	Virtual Asset Service Provider (VASP)
Regulation	Part 4 of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI)	Part 9 of the MORNBFI
Related Circulars	Circular No. 649, Circular No. 942	Circular No. 942, Circular No. 944, Circular No. 1108
Definition	An EMI provides money transfer or remittance services using electronically stored money value system and similar digital financial services.	VASP refers to any entity that offers services or engages in activities that provide facility for the transfer or exchange of virtual assets, which involve the conduct of one or more of the following activities: (1) exchange between VAs and fiat currencies; (2) exchange between one or more forms of VAs; (3) transfer of VAs; and (4) safekeeping and/or administration of VAs or instruments enabling control over VAs.
Product / Service	e-money, e-wallets	virtual assets/currencies (Bitcoin, Ethereum, Ripple, etc.), e-wallets

² Full list of registered EMIs and VCE/VASPs can be found in the BSP website.

Will the BSP regulate Initial Coin Offerings (ICO)?

The BSP's guidelines do not cover businesses involved in the participation and provision of financial services related to an issuer's offer and/or sale of a VA. Initial Coin Offerings or ICOs are under the regulatory purview of the Securities and Exchange Commission (SEC).

According to the SEC Proposed Rules on Initial Coin Offerings, ICOs or token sales are defined as distributed ledger technology fundraising operations involving the issuance of tokens in return for cash, other cryptocurrencies or other assets. They involve coins (or "tokens") being issued in order to raise money from the general public. Once the project reaches a certain stage, benefits to tokenholders may include, but is not limited to, any of the following:

- a. **Gains through profits or increase in the value of tokens which can be sold if the project is successful;**
- b. **Voting or governance rights; or**
- c. **Usage rights.**

What security features are required for VASPs?

VASPs are expected to comply with the requirements of BSP Circular No. 808 on Information Technology Risk Management and BSP Circular No. 982 covering the Enhanced Guidelines on Information Security Management for BSP-Supervised Financial Institutions (BSFIs).

Moreover, VASPs providing wallet services for holding and storing VAs must establish an adequate cybersecurity framework and adopt appropriate security measures/controls in its VA platform to ensure confidentiality, integrity and availability of data/information uploaded, stored, processed and transmitted into and out of the system and protect the infrastructure from malware, cyber-attacks and other evolving and emerging threats. They are required to employ appropriate security mechanisms commensurate to the sensitivity and criticality of applications used. This may include robust authentication methods in offering their products and services, such as multi-factor authentication. VASPs are expected to conduct at least an annual vulnerability assessment and penetration tests, as well as application security tests to ensure applications and platforms meet the desired level of security.

These security-related regulations are periodically updated in response to the dynamically evolving security, regulatory, and business environment where VASPs operate.

How do clients go about complaints processing in cases where they experience any issues with VASPs?

VASPs are required to set up customer awareness measures to educate its customers, which includes, among others: (i) safeguarding of VA and/or fiat currency wallets as well as protection of client information such as log-in credentials; (ii) use of the mobile platform

and wallets; (iii) actual fees and charges related to the use of the mobile platform and withdrawal transactions; and (iv) problem resolution procedures.

VASPs shall clearly communicate and explain to its customers the terms and conditions prescribing the manner on how the losses and liabilities from security breaches, system failure, or human error will be settled between the VASP and its customers.

Clients/Users, on the other hand, should be aware of the risks involved in transacting or engaging in the use of VA. As such, they should take full responsibility of their virtual/electronic wallets, VAs, and transactions with VASPs. Should clients/user experience any issues with VASPs, they should first directly communicate with the VASP through their hotlines, emails, or available contact information to raise any concerns with regard to using their product/service. Nevertheless, they may raise their concerns to the BSP by following the instructions posted in the BSP's Consumer Assistance Channels and Chatbot page. (<https://www.bsp.gov.ph/Pages/InclusiveFinance/ConsumerAssistanceChannelsChatbot.asp>). Any issues received from the public will be duly attended and communicated to the erring VASP. Reported complaints shall be closely monitored with the VASP until full resolution.

How can an entity obtain a Certificate of Authority (COA) to operate as a VASP?

For new applications, entities may refer to the existing registration process for EMIs/VCEs as provided in the 2020 BSP Citizen's Charter.

For VCEs (now referred to as VASP) with existing Certificate of Registration (COR), a letter of intent (LOI) and gap assessment may be submitted to trisd@bsp.gov.ph with the subject: **DDMMYYYY_VASP LOI_Name of Entity**. Submission must be made within three (3) months from the effectivity date of subject Circular or 16 May 2021.

Note: DDMMYYYY refers to the date of submission