EMAIL SUBMISSION TO:

To whom it may concern,

Re: Taiwan - Financial Supervisory Commission Announcement: Preview of the "Virtual Asset Services Act"

About Global Digital Finance (GDF)

GDF is the leading global members association advocating and accelerating the adoption of best practices for crypto and digital assets. GDF's mission is to promote and facilitate greater adoption of market standards for digital assets through the development of best practices and governance standards by convening industry, policymakers, and regulators.

The input to this response has been curated through a series of member discussions, industry engagement, and previous engagement with global regulators over the years and GDF is grateful to its members who have taken part.

As always, GDF remains at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail with our members.

Yours faithfully,
Elise Soucie Watts – Executive Director – GDF

Response to the Consultation: Executive Summary

GDF convened our APAC Policy and Regulatory Working Group to analyse the Taiwanese Consultation, **Preview of the "Virtual Asset Services Act",** published by the Financial Supervisory Commission (FSC). Please note that as this response was developed in collaboration with GDF members, as well as community partners, that portions of our response may be similar or verbatim to individual member responses.

Overall, we believe that the development of the Virtual Asset Services Act (referred to henceforth as 'VASA') is a welcome step forward. In our comments GDF wished to call attention to several important considerations for Taiwanese regulators as they work to build a framework for virtual assets, chiefly with regards to **market size and influence, proportionality scope, and global considerations from market participants who have engaged with other jurisdictional regimes.** Throughout the response we expand on these key themes aiming to highlight key areas where more consideration should be given to the unique innovations within digital asset markets, as well as evolving regulations in both other jurisdictions as well as from global standard setters. Global best practice and the advances happening both in industry and in other fast-moving jurisdictions can help to frame a Taiwanese approach.

We also appreciate the opportunity to engage on the proposals. Through our process of working with our members we identified key thematic areas that we believe the FSC should consider as they move forward to develop a regulatory regime. The key themes identified are:

1. We support greater alignment to FATF standards and definitions wherever possible;

2. We support the development of proportionate, evidence based, consumer protection, financial crime, market integrity and financial stability solutions as the industry and technology continues to mature;

3. We request that access to global liquidity be carefully evaluated and that the Securities and Futures Bureau of the Financial Supervision Commission consider the benefits of global liquidity holistically and on a case-by-case basis; and

4. While we appreciate the consideration of global frameworks like MiCA, we believe that Taiwan could take a more nuanced approach specific to their own market.

Response to the Proposals

Comments on Scope

Overall, we believe that Virtual Assets should be governed under a regulatory framework appropriate for the unique risks and opportunities presented by Virtual Assets. Furthermore, we also believe that the proposed regulatory framework should apply to: Virtual Asset Service Providers (VASP) and issuers of Virtual Assets, including stablecoins. Our comments below aim to reframe the scope in a way that is consistent with global definitions and provisions, and specifically in alignment with the Financial Action Taskforce (FATF);

Virtual Asset Service Provider: The FATF defines Virtual Asset Service Providers as firms that provide any of the following services relating to Virtual Assets:

- exchange between Virtual Assets and fiat currencies;
- exchange between one or more forms of Virtual Assets;
- transfer of Virtual Assets, that is to say, to conduct a transaction on behalf of another person that moves a Virtual Asset from one Virtual Asset address or account to another;
- custodian wallet provider; and
- participation in, and provision of, financial services related to an issuer's offer or sale of a Virtual Asset or both.

Virtual Asset: The FATF defines a Virtual Asset as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual Assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere (in the FATF Recommendations)[1]. This approach is consistent with FATF's Updated Guidance[2], which notes that a "Virtual Asset that is exchangeable for another asset, such as a stablecoin that is exchangeable for a fiat currency or a Virtual Asset at a stable rate" will be a Virtual Asset providing it is considered to have "inherent value to be traded or transferred and used for payment", rather than just being a record of ownership of something else.

We would recommend that the VASA aim to align with FATF as much as possible in their new requirements for Virtual Assets. Globally consistent terminology is critical, and definitions based on Global Standard-Setting Bodies and international best practices (e.g., Financial Action Task Force ("FATF")) would be most welcome.

Comments on Proportionality

GDF firmly believes that proportionate and appropriate regulation is an important part of the lifecycle of all innovative sectors to help foster innovation and continue to provide users with access to new, world-changing innovations. The foundation of such a regulatory framework should be built on basic principles to maximise protections for consumers and firms by fostering a safe, secure and sustainable digital ecosystem.

Governments ultimately determine which institutions have oversight over Virtual Assets within countries. Wherever possible terminology should be consistent across all regulatory frameworks, and it should also be technologically neutral and supportive of responsible innovation.

Particular consideration should be given to proportionate, evidence based, consumer protection, financial crime, market integrity and financial stability solutions as the industry and technology continues to mature. There is a risk that disproportionate regulation that has an outsized focus protecting consumers and markets may inadvertently stifle innovation and growth, remove choice and competition, and drive consumers to unregulated markets or operators. Done well, responsible operators can facilitate appropriate solutions and help

[1] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (see Glossary)

[2] 2019 Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (VASPs).

countries and policymakers to achieve their own objectives, whilst also providing choice and opportunity for their citizens and markets.

Comments on Liquidity

GDF would request that access to global liquidity be carefully evaluated and that the Securities and Futures Bureau of the Financial Supervision Commission consider the benefits of global liquidity holistically and on a case-by-case basis. In many jurisdictions, including the EU, there are no specific regulatory prohibitions against using a global order book.

We believe that a large liquidity pool is one of the best consumer protection mechanisms. It protects against market manipulation, volatility and reduces liquidations.

Large liquidity pools also provide better prices for users, tighter spread and lower slippage, directly benefiting users from a financial perspective. On crypto exchanges, users trade on the orderbook i.e., they do not know the identity of their counterparty or counterparties, which is/are determined by automatic matching (meaning there is no execution risk).

Given the important role of liquidity in maintaining market stability and efficiency, licensed virtual asset exchanges should be permitted to retain their global liquidity pools, rather than being required to segregate orders by jurisdiction. In the medium to long-term, fragmented liquidity would make trading more expensive, reduce competition and restrict innovation.

Global Considerations

We would note that the draft VASA appears to heavily reference the Markets in Crypto-Assets (MiCA) framework of Europe. While this is understandable given MiCA's comprehensive and solid nature, there are several important considerations for Taiwanese regulators:

a. **Market Size and Influence:** The European Union (EU) market is significantly larger, approximately 15-20 times the size of Taiwan's market. Consequently, EU regulations often require companies to make substantial investments in local resources to comply with stringent requirements. Taiwanese regulators should consider the scalability and applicability of such demands within the context of Taiwan's market size and economic capacity.
b. **Building on EU Regulatory Experience:** GDF and our members have supported the EU crypto-assets policy process actively. As such, we note that the EU experience, and the broader global policy experience of jurisdictions such as Singapore, the UAE, UK and the US demonstrate that from the drafting period of MiCA (up to September 2020) to today, the crypto industry has significantly evolved. As such, we encourage the Taiwanese authorities to learn from the broader global experience and most recent regulatory thinking.
c. **EU/MiCA Special Context:** MiCA was developed within a unique European context, addressing specific challenges and regulatory needs pertinent to the EU. These include harmonizing regulations across diverse member states and addressing cross-border financial activities. Taiwanese regulators should assess whether these contextual factors align with Taiwan's regulatory environment and economic objectives, ensuring that any adoption of MiCA-like frameworks is tailored to local needs and conditions.

GDF would also encourage consideration of how to integrate global standards for technology and data governance for matters such as market surveillance. We would highlight for example the IOSCO principles as an example of such standards. We believe aligning to global principles where possible is beneficial for consistency in both supervision as well as firms' ability to meet regulatory expectations.

Article Specific Comments

Article 25: *Virtual asset trading platform operators shall establish review standards and review procedures for the listing and delisting of virtual assets in accordance with the regulations of the competent authorities.*

Virtual asset trading platform operators shall not provide services under Article 6, Paragraph 2, Subparagraph 2 involving virtual assets that have not been approved by the competent authority.

The procedures for applying for approval and other matters to be complied with shall be prescribed by the competent authority. Virtual asset trading platform operators should establish mechanisms to prevent unfair market transactions and measures such as detecting abnormal price and volume warnings.

The provisions of the preceding article shall also apply to virtual asset trading platform operators.

Response:

Global policy examples, including from the EU and from the UAE, as well as supervisory learnings from these jurisdictions point out that when a Competent Authority is required to approve each Virtual Asset listed on domestic exchanges, both bottlenecks appear on the market and domestic consumers solicit offshore services. The two outcomes are interlinked.

To this end, usually the responsibility for due diligence on listed Virtual Assets is shared by the VA firms and the VA issuers by way of a simplified white paper notification procedure (e.g., in MiCA).

We believe that it is a Regulated VA Firm's responsibility to ensure the business of the firm is controlled effectively, that the business complies with regulatory requirements and that any delegation of responsibilities is appropriate and properly overseen. The arrangements should be comprehensive and proportionate to the nature, scale and complexity of the risks inherent in the business model and of the firm's activities. This should include the procedure for assessing and listing VAs.

Given the expertise of VA exchanges in assessing new crypto projects a Regulated VA Firm should be primarily responsible for ensuring that it is satisfied that the VA seeking admission is acceptable, and for devising its own internal policies and procedures for reaching that conclusion. This approach is similar to that adopted globally for admission of derivatives to trading.

We believe that it is important to consider appropriate regulatory oversight of the admission

process to trading VAs on exchanges, whilst balancing the responsibilities of the Regulated VA Firm and the Securities and Futures Bureau of the Financial Supervision Commission. In our view this can be achieved if the Regulated VA Firm self-certifies by notifying the relevant competent regulator "ex-post" that the VA it has listed is acceptable, and that it has met the Regulated VA Firm's requirements for Listing.

Regulators could also publish a list of all acceptable VAs submitted to it. The publication of such a list would provide certainty to the industry as to which products are acceptable. This would be of particular assistance to new or developing exchanges and would provide users with additional comfort that the VAs they are buying or selling are regulated products.

Article 27: *Where a virtual asset custodian entrusts another person to keep a client's virtual assets, such other person shall be limited to a virtual asset custodian permitted by the competent authority. Virtual asset custodians shall inform customers of the circumstances set forth in the preceding paragraph.*

Response:
The Financial Stability Board's recent consultation on "Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets " identified in its Annex 1 "Essential functions, risks and relevant international standards" that Function 2: Wallets and custody are operational risks (please refer to Annex I)

In this context, we would like to suggest the following:

That the proportion and mix of VAs in hot and cold wallets is dependent on the VASPs business model and should be managed in line with, for example, its liquidity risk management policy and processes to ensure good operational resilience. This proportion and mix should be managed operationally and not mandated by the Securities and Futures Bureau of the Financial Supervision Commission. For example, mandating a small upper limit on the overall volume of VAs that are able to be stored in a VASP's hot wallet (e.g., 10 percent) could (i) impact the speed at which customer withdrawals can take place; (ii) compromise security systems of the VASP as it will require more sweeping from the cold to the hot wallet.

Recent examples of VA exploits clearly demonstrate that the reliance on cold storage is not, in itself, a sufficient security posture. On the contrary, prescriptive cold storage requirements create a false sense of security in supervised entities and deflect supervisory and industry attention from a number of attack vectors, such as access rights, to which the offline environment is as vulnerable as the online environment.

Instead, operational resilience for the VA custody function should require an end-to-end security architecture with the following five elements: (i) cybersecurity, (ii) privileges and access management, (iii) detection, response, and investigation management, (iv) business continuity, disaster recovery, resolvability, and (v) key management.

In addition to having risk management controls for the storage of private keys, having such controls for the key generation process is also critical to safeguard private keys as private keys may be subjected to single points of failure, as well as internal or external threats. As such, we want to suggest the use of Multi Party Computation (MPC) in key generation, which is a mechanism to generate and split the private key into multiple pieces distributing them in

multiple places and storing them securely so that no one person will have full access to the private key. This methodology, in our view, has superior risk controls against the traditional method of creating private keys.

We would also suggest that where a third-party, whether an external service provider or an intra-group entity, only provides technology solutions but not regulated activities or services, then this third-party should not require formal approval/authorisation from the competent authority. In such circumstances, we would propose that the third-party entity should be subject to third party outsourcing requirements.