Staff Accounting Bulletin No. 121: Safeguarding Crypto Assets

OVERVIEW

On March 31, 2022, the SEC issued Staff Accounting Bulletin No. 121 (SAB 121), which expresses the SEC staff's views on accounting for an entity's obligations to safeguard crypto assets for another party. Safeguarding crypto assets presents unique risks and uncertainties, including technological, legal and regulatory risks. In the SEC staff's views, the objective of SAB 121 is to "enhance the information received by investors and other users of financial statements about these risks, thereby assisting them in making investment and other capital allocation decisions."

This publication includes key considerations on scope, recognition, measurement, disclosure, and adoption of SAB 121, as well as on internal control over financial reporting (ICFR) related to SAB 121.

The AICPA also updated its AICPA Practice Aid, *Accounting for and auditing of digital assets* (AICPA Practice Aid) to add Appendix B, which includes insights in a Question and Answer (Q&A) format on applying SAB 121 based on recent discussions with the SEC staff. We strongly recommend that entities consider the information in Appendix B when applying SAB 121.

SCOPE

SAB 121 defines a crypto asset[1] as "a digital asset that is issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques." This definition of a crypto asset is broad and is not limited to cryptocurrencies (e.g., Bitcoin, Ether) that are fungible and used as a medium of exchange. Rather, under this definition, crypto assets can also include stablecoins and non-fungible tokens that exist on the blockchain.

SAB 121 applies to all entities that file financial information with the SEC under U.S. GAAP or International Financial Reporting Standards and that have a safeguarding obligation for crypto assets. However, as discussed in Q&A 4 of the AIPCA Practice Aid, if an entity controls the crypto assets and therefore recognizes them on its balance sheet, the entity does not apply SAB 121 to those crypto assets.

Entities that file financial information with the SEC include the following:

- Entities that file reports under Section 13(a) or Section 15(d) of the Securities Exchange Act of 1934 (Exchange Act) and periodic and current reports under Rule 257(b) of Regulation A (SEC Filers)
- Entities that have submitted or filed a registration statement under the Securities Act of 1933 or the Exchange Act that is not yet effective
- Entities that are in the process of submitting or filing an offering statement or post-qualification amendment under Regulation A
- Entities whose financial statements are filed with the SEC in accordance with Rule 3-09 and 3-05 of Regulation S-X
- Private operating entities whose financial statements are included in filings with the SEC in connection with a business combination involving a shell company, including a special purpose acquisition company

[1] The definition of "crypto asset" in SAB 121 differs from definitions used by the following organizations: American Institute of Certified Public Accountants, Financial Accounting Standards Board and Internal Revenue Service. Refer to hyperlinks for each organization's definition.

SAB 121 does not say how to determine whether an entity has a safeguarding obligation for crypto assets. SAB 121 includes an example of an entity that safeguards crypto assets held for its platform users and concludes that the entity's safeguarding activities are in scope of SAB 121. However, an entity is not required to operate a platform to be in the scope of SAB 121, as discussed in Q&A 3 in Appendix B of the AICPA Practice Aid. Further, an entity that is acting as an agent on behalf of another entity may be required to apply SAB 121. In such cases, there may be multiple entities in the arrangement that each must apply SAB 121.

Implied promises and perceptions of responsibilities for safeguarding crypto assets may override explicit provisions in agreements intended to limit an entity's risks on safeguarding crypto assets. For example, a custodial or wallet agreement may include explicit provisions that limit or disclaim the custodian's liability if the user is a victim of fraud or theft resulting in the loss of crypto assets. However, even so, a custodian could still be exposed to safeguarding risks (and therefore could have a safeguarding obligation) despite the explicit provision in the agreement that is intended to alleviate or mitigate such risks because of the lack of legal precedent on the enforceability of such provisions as well as a perceived view by users that the custodian is the safeguarding obligor and thus responsible for losses.

BDO Insight

The determination of whether an entity has a safeguarding obligation under SAB 121 depends on facts and circumstances and may require significant judgment. Q&A 7 in Appendix B of the AICPA Practice Aid includes a list (although not exhaustive) of factors to consider in this determination. If, after considering the entity's facts and circumstances and the factors in Q&A 7, there is still uncertainty about whether SAB 121 applies, consider consulting with an accounting or legal advisor..

RECOGNITION AND MEASUREMENT

Under SAB 121, if an entity is responsible for safeguarding crypto assets, it recognizes a liability on its balance sheet for its safeguarding obligation. The entity also recognizes a corresponding asset similar to an indemnification asset under ASC 805, *Business Combinations*. The safeguarding asset and liability are initially measured at the fair value of the crypto assets. Changes in the fair value of the safeguarding asset and liability may be recorded within the same line item in the income statement. If such changes in the fair value of the safeguarding asset and liability are recognized for the same amount in the same reporting period, there is no effect on the income statement, which will always be the case absent a safeguarding loss.

However, upon a safeguarding loss, an entity recognizes a loss on the safeguarding asset without recognizing a corresponding change in the liability, which results in a net loss in income from operations for the difference. For example, assume the fair value of safeguarded crypto assets is initially $300,000. Subsequently, a user's wallet was 'hacked' and its crypto assets were stolen, which was 1% (or $3,000) of all safeguarded crypto assets. The safeguarding asset is reduced by $3,000 and recognized as a loss in income from operations. Assuming the fair value of the crypto assets being safeguarded is still $300,000, the balance of the safeguarding asset is $297,000, and the balance of the safeguarding liability remains $300,000.

DISCLOSURE

SAB 121 provides the SEC staff's views on disclosures to include in the notes to the financial statements due to the significant risks and uncertainties associated with safeguarding crypto assets, including risk of loss. At a minimum, the disclosures should include:

- Nature and amount of crypto assets that the entity is safeguarding, with separate disclosure for each significant crypto asset
- Vulnerabilities due to any concentrations in such safeguarding activities

- Fair value disclosures required under ASC 820, *Fair Value Measurement*, for the safeguarding asset and liability
- Accounting for the safeguarding asset and liability
- Information about who is responsible for the recordkeeping of the crypto assets, holding of the cryptographic keys to access the crypto assets and safeguarding the crypto assets from loss or theft

In addition, the SEC staff indicated that entities may need to consider including disclosures outside the financial statements (e.g., MD&A). Refer to interpretive response to Question 2 of SAB 121 for examples of these disclosures.

ADOPTION

SAB 121 applies to SEC Filers no later than the first interim or annual period ending **after** June 15, 2022, with retrospective application as of the beginning of the fiscal year to which the interim and annual period is related. For calendar year-end companies, this date was no later than the interim financial statements for the period ended June 30, 2022, with retrospective application as of January 1, 2022.

For all other entities[2], SAB 121 is applicable to an entity's financial statements beginning with the next submission or filing with the SEC, with retrospective application as follows:

Effective Date	Example
As of the beginning of the most recent annual period ending *before* June 15, 2022, if the filing also includes a subsequent interim period reflecting application of SAB 121.	Calendar year-end entity A submits a registration statement in January 2023. Such filing includes interim financial statements for the period ended September 30, 2022, in which SAB 121 was applied. SAB 121 also applies to the annual financial statements ended December 31, 2021.
As of the beginning of the two most recent annual periods ending *before* June 15, 2022, if the filing does not include a subsequent interim period reflecting application of SAB 121.	Calendar year-end entity B submitted a registration statement in April 2022. That filing did not include any interim financial statements reflecting application of SAB 121. SAB 121 applied to the annual financial statements ended December 31, 2021, and 2020.

INTERNAL CONTROL OVER FINANCIAL REPORTING

While entities adopting SAB 121 must focus on getting the numbers right in their financial statements, they should not overlook the internal controls necessary to comply with its requirements. Maintaining appropriate controls over the information used to recognize and measure the safeguarding asset and liability and make the required disclosures is critical, even for private companies that do not obtain an audit of internal controls over financial reporting, given complexities that may be present regarding the nature of, and the methods used to store, crypto assets. Regardless of the accounting system or underlying spreadsheets used by management, if there are not effective internal controls over the completeness and existence of safeguarding assets and obligations, accuracy of the underlying data,

[2] Includes entities that have submitted or filed a registration statement under the Securities Act of 1933 or the Exchange Act that is not yet effective or that are in the process of submitting or filing an offering statement or post-qualification amendment under Regulation A, as well as private operating entities whose financial statements are included in filings with the SEC in connection with a business combination involving a shell company, including a special purpose acquisition company.

and valuation of crypto assets, risks to the financial statements (and to the business) could be unmitigated.

Each entity should evaluate its unique inherent risks and design and implement effective internal controls to address those risks. This evaluation may include assessing the design and operating effectiveness of controls of service providers and sub-service providers (e.g., sub-custodians). In addition, management should consider whether it stores assets safeguarded on behalf of others in commingled public addresses, including whether the assets are commingled with the entity's own assets, and if so, design controls to address the increased risk associated with that practice.

Examples of relevant controls include:

- Entity-level controls over risk assessments to identify and respond to new risks (Committee of Sponsoring Organizations Principle 9)
- Review of accounting policies over the appropriate recognition, measurement, presentation, and disclosure guidance to apply
- IT and business process controls over:
  - Securing and controlling an entity's private keys (see our publication Accounting for the Purchase, Sale and Receipt of Cryptocurrencies for more guidance)
  - Tracking and reconciling crypto assets held on behalf of others (in segregated or commingled public addresses) between the blockchain and internal books and records
  - Tracking customer fund flows, including the timeliness of crypto asset purchases and sales
  - Measuring safeguarding assets and obligations (determining the fair value of the underlying crypto assets)
  - Identifying and measuring safeguarding losses on a timely basis
  - Providing appropriate disclosures
- Service organization controls, including relevant sub-service providers, and relevant complimentary user entity controls - Refer to AU-C Section 402 – *Audit Consideration of an Entity's Use of a Service Organization* for more information.

Executive oversight of an entity's internal controls, stakeholder training and communication are critical to successfully applying the guidance in SAB 121. As part of those responsibilities, management and those charged with governance (e.g., audit committees) should understand the plan for compliance with SAB 121 and confirm that the entity's controls adequately address these unique risks.