
Staff Accounting Bulletin No. 121

SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 211

[Release No. SAB 121]

Staff Accounting Bulletin No. 121

AGENCY: Securities and Exchange Commission.

ACTION: Publication of Staff Accounting Bulletin.

SUMMARY: This staff accounting bulletin expresses the views of the staff regarding the accounting for obligations to safeguard crypto-assets an entity holds for platform users.

EFFECTIVE DATE: Effective [Insert date of publication in the Federal Register.]

FOR FURTHER INFORMATION CONTACT: The Office of the Chief Accountant at (202) 551-5300, or the Division of Corporation Finance's Office of the Chief Accountant, at (202) 551-3400, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION:

The statements in staff accounting bulletins are not rules or interpretations of the Commission, nor are they published as bearing the Commission's official approval. They represent staff interpretations and practices followed by the staff in the Division of Corporation Finance and the Office of the Chief Accountant in administering the disclosure requirements of the federal securities laws.

Dated:

Vanessa Countryman
Secretary

March 31, 2022

PART 211 — [AMENDED]

Accordingly, Part 211 of Title 17 of the Code of Federal Regulations is amended as follows:

PART 211—INTERPRETATIONS RELATING TO FINANCIAL REPORTING MATTERS

1. The authority citation for 17 CFR 211 continues to read as follows: Authority: 15 U.S.C. 77g, 15 U.S.C. 77s(a), 15 U.S.C. 77aa(25) and (26), 15 U.S.C. 78c(b), 15 U.S.C. 78l(b), 15 U.S.C. 78m(b), 15 U.S.C. 80a-8, 15 U.S.C. 80a-29(e), 15 U.S.C. 80a-30, and 15 U.S.C. 80a-37(a).
2. Amend the table in subpart B by adding an entry for Staff Accounting Bulletin No. 121 at the end of the table to read as follows:

Subpart B—Staff Accounting Bulletins

Subject

Release No.

Date

Fed. Reg. Vol. and page

* * * * *

Publication of Staff Accounting Bulletin No. 121

SAB121

[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]

[INSERT FEDERAL REGISTER CITATION]

Note: The text of Staff Accounting Bulletin No. 121 will not appear in the Code of Federal Regulations.

Staff Accounting Bulletin No. 121

The staff hereby adds Section FF to Topic 5 of the Staff Accounting Bulletin Series. This staff accounting bulletin (“SAB”) adds interpretive guidance for entities to consider when they have obligations to safeguard crypto-assets held for their platform users. This SAB is applicable to entities that file reports pursuant to Sections 13(a) or 15(d) of the Securities Exchange Act of 1934 (“Exchange Act”) and entities that have submitted or filed a registration statement under the Securities Act of 1933 (“Securities Act”) or the Exchange Act that is not yet effective. The SAB is also applicable to entities submitting or filing an offering statement or post-qualification amendment thereto under Regulation A, entities subject to the periodic and the current reporting requirements of Regulation A, and private operating companies 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. Accordingly, the staff hereby amends the Staff Accounting Bulletin Series as follows:

TOPIC 5: Miscellaneous Accounting

The interpretations in this SAB express views of the staff regarding the accounting for entities that have obligations to safeguard crypto-assets held for their platform users.^[1] In recent years, the staff has observed an increase in the number of entities that provide platform users with the ability to transact in crypto-assets. In connection with these services, these entities and/or their agents may safeguard the platform user’s crypto-asset(s) and also maintain the cryptographic key information necessary to access the crypto-asset. The obligations associated with these arrangements involve unique risks and uncertainties not present in

arrangements to safeguard assets that are not crypto-assets, including technological, legal, and regulatory risks and uncertainties. Specifically:

- **Technological risks** – there are risks with respect to both safeguarding of assets and rapidly-changing crypto-assets in the market that are not present with other arrangements to safeguard assets for third parties;
- **Legal risks** – due to the unique characteristics of the assets and the lack of legal precedent, there are significant legal questions surrounding how such arrangements would be treated in a court proceeding arising from an adverse event (e.g., fraud, loss, theft, or bankruptcy); and
- **Regulatory risks** – as compared to many common arrangements to safeguard assets for third parties, there are significantly fewer regulatory requirements for holding crypto-assets for platform users or entities may not be complying with regulatory requirements that do apply, which results in increased risks to investors in these entities.

These risks can have a significant impact on the entity's operations and financial condition. The staff believes that the recognition, measurement, and disclosure guidance in this SAB will 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.

FF. Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users

Facts: Entity A's^[2] business includes operating a platform that allows its users to transact in crypto-assets.^[3] Entity A also provides a service where it will safeguard the platform users' crypto-assets,^[4] including maintaining the cryptographic key information^[5] necessary to access the crypto-assets. Entity A also maintains internal recordkeeping of the amount of crypto-assets held for the benefit of each platform user. Entity A secures these crypto-assets and protects them from loss or theft, and any failure to do so exposes Entity A to significant risks, including a risk of financial loss. The platform users have the right to request that Entity A transact in the crypto-asset on the user's behalf (e.g., to sell the crypto-asset and provide the user with the fiat currency (cash) proceeds associated with the sale) or to transfer the crypto-asset to a digital wallet for which Entity A does not maintain the cryptographic key information. However, execution and settlement of transactions involving the platform users' crypto-assets may depend on actions taken by Entity A.

Question 1: How should Entity A account for its obligations to safeguard crypto-assets held for platform users?

Interpretive Response: The ability of Entity A's platform users to obtain future benefits from crypto-assets in digital wallets where Entity A holds the cryptographic key information is dependent on the actions of Entity A to safeguard the assets. Those actions include securing the crypto-assets and the associated cryptographic key information and protecting them from loss, theft, or other misuse. The technological mechanisms supporting how crypto-assets are issued, held, or transferred, as well as legal uncertainties regarding holding crypto-assets for others, create significant increased risks to Entity A, including an increased risk of financial loss.^[6] Accordingly, as long as Entity A is responsible for safeguarding the crypto-assets held for its platform users, including maintaining the cryptographic key information necessary to access the crypto-assets, the staff believes that Entity A should present a liability on its balance sheet to reflect its obligation to safeguard the crypto-assets held for its platform users.

As Entity A's loss exposure is based on the significant risks associated with safeguarding the crypto-assets held for its platform users, the staff believes it would be appropriate to measure this safeguarding liability at initial recognition and each reporting date at the fair value^[7] of the crypto-assets that Entity A is responsible for holding for its platform users. The staff also believes it would be appropriate for Entity A to recognize an asset^[8] at the same time that it recognizes the safeguarding liability, measured at initial recognition and each reporting date at the fair value of the crypto-assets held for its platform users.^[9]

Question 2: Assume the same facts as Question 1. What disclosures would the staff expect Entity A to provide regarding its safeguarding obligations for crypto-assets held for its platform users?

Interpretive Response: In light of the significant risks and uncertainties associated with safeguarding crypto-assets, including the risks of loss associated with holding the cryptographic key information necessary to

secure and transact in the crypto-asset, the staff believes the notes to the financial statements should include clear disclosure of the nature and amount of crypto-assets that Entity A is responsible for holding for its platform users, with separate disclosure for each significant crypto-asset, and the vulnerabilities Entity A has due to any concentration in such activities.^[10] In addition, because the crypto-asset safeguarding liabilities and the corresponding assets are measured at the fair value of the crypto-assets held for its platform users, the entity would be required to include disclosures regarding fair value measurements.^[11] The accounting for the liabilities and corresponding assets should be described in the footnotes to the financial statements.^[12] In providing these disclosures, Entity A should consider disclosure about who (e.g., the company, its agent, or another third party) holds the cryptographic key information, maintains the internal recordkeeping of those assets, and is obligated to secure the assets and protect them from loss or theft.

Disclosures regarding the significant risks and uncertainties associated with the entity holding crypto-assets for its platform users may also be required outside the financial statements under existing Commission rules, such as in the description of business, risk factors, or management's discussion and analysis of financial condition and results of operation.^[13] For example, to the extent it is material, Entity A may need to provide disclosure describing the types of loss or additional obligations that could occur, including customer or user discontinuation or reduction of use of services, litigation, reputational harm, and regulatory enforcement actions and additional restrictions. A discussion of the analysis of the legal ownership of the crypto-assets held for platform users, including whether they would be available to satisfy general creditor claims in the event of a bankruptcy should be considered. Further, Entity A may need to provide disclosure of the potential impact that the destruction, loss, theft, or compromise or unavailability of the cryptographic key information would have to the ongoing business, financial condition, operating results, and cash flows of the entity. As part of this disclosure, Entity A should also consider including, to the extent material, information about risk-mitigation steps the entity has put in place (e.g., insurance coverage directly related to the crypto-assets held for platform users).

Question 3: How and when should Company A initially apply the guidance in this Topic in its financial statements?

Interpretive Response: The staff would expect an entity that files reports pursuant to Section 13(a) or Section 15(d) of the Exchange Act, or an entity required to file periodic and current reports pursuant to Rule 257(b) of Regulation A, to apply the guidance in Topic 5.FF no later than its financial statements covering 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 or annual period relates.

The staff expects all other entities, including but not limited to entities conducting an initial registration of securities under the Securities Act or Exchange Act, entities conducting an offering of securities under Regulation A, and private operating companies entering into a business combination transaction with a shell company, including a special purpose acquisition company, to apply the guidance in Topic 5.FF beginning with their next submission or filing with the SEC (e.g., the initial or next amendment of the registration statement, proxy statement, or Form 1-A), with retrospective application, at a minimum, as of the beginning of the most recent annual period ending before June 15, 2022, provided the filing also includes a subsequent interim period that also reflects application of this guidance.^[14] If the filing does not include a subsequent interim period that also reflects application of this guidance, then the staff expects it to be applied retrospectively to the beginning of the two most recent annual periods ending before June 15, 2022.

For all entities, in the financial statements that reflect the initial application of this guidance, the effect of the initial application should be reported in the carrying amounts of assets and liabilities as of the beginning of the annual period specified above. Entities should include clear disclosure of the effects of the initial application of this guidance.^[15]

^[1] This SAB expresses no view with respect to any other questions that these activities may raise for any of the entities involved, including the applicability of the registration or other provisions of the federal securities laws or any other federal, state, or foreign laws.

- [2] References throughout this SAB to “Entity A” are inclusive of the entity as well as any agent acting on its behalf in safeguarding the platform users’ crypto-assets.
- [3] For purposes of this SAB, the term “crypto-asset” refers to a digital asset that is issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques.
- [4] The service may be provided by Entity A or by an agent acting on Entity A’s behalf.
- [5] The guidance in this SAB is applicable regardless of whether the cryptographic key remains in the name of the platform user or is in the name of the Entity.
- [6] See *generally* Report of the Attorney General’s Cyber Digital Task Force: Cryptocurrency Enforcement Framework (Oct. 2020), at 15-16, available at <https://www.justice.gov/ag/page/file/1326061/download>.
- [7] For U.S. generally accepted accounting principles (“U.S. GAAP”), refer to glossary definition provided in Financial Accounting Standards Board (“FASB”) Accounting Standards Codification (“ASC”) Topic 820. For International Financial Reporting Standards (“IFRS”), refer to glossary definition provided in IFRS 13.
- [8] The asset recognized is similar in nature to an indemnification asset as described in FASB ASC 805 and IFRS 3. The measurement of the asset is on the same basis as the crypto-asset safeguarding liability assumed by the entity. The asset recognized by the entity is separate and distinct from the crypto-asset itself that has been transferred to and then held for the platform user.
- [9] Similar to the guidance in FASB ASC 805 and IFRS 3, Entity A would need to evaluate whether any potential loss events, such as theft, impact the measurement of the asset.
- [10] For U.S. GAAP, see FASB ASC 275-10-50. For IFRS, see IAS 1.
- [11] For U.S. GAAP, see FASB ASC 820. For IFRS, see IFRS 13.
- [12] For U.S. GAAP, see FASB ASC 235-10-50. For IFRS, see IAS 1.
- [13] See, e.g., Item 101 of Regulation S-K; Item 105 of Regulation S-K; Item 303 of Regulation S-K.
- [14] For example, a calendar year-end company that submits a registration statement in January 2023 including financial statements as of and for the fiscal year ending December 31, 2021 and as of and for the nine months ended September 30, 2022 would apply the SAB to those periods.
- [15] For U.S. GAAP, see FASB ASC 250-10-50-1 through 50-3; for IFRS, see IAS 8. See *also*, e.g., Item 302 of Regulation S-K and PCAOB Auditing Standard 2820 (par. 8).

Modified: March 31, 2022