

**What's inside**

Background.....1

Appendix.....2

    3.7 Accounting for obligations to safeguard crypto assets.....2

    5.2 SAB 121: presentation and disclosure.....7

**At a glance**

The SEC staff has released interpretive guidance in SAB 121 requiring reporting entities that perform custodial activities related to crypto assets to include a crypto asset safeguarding liability and a corresponding asset on their balance sheets at fair value. This *In depth* addresses the accounting and disclosure-related impacts of SAB 121.

## Background

In March 2022, the SEC staff released [Staff Accounting Bulletin No. 121 \(SAB 121\)](#), which provides interpretive guidance for reporting entities that engage in activities in which they have an obligation to safeguard customers' crypto assets. The guidance is applicable to certain reporting entities that apply US GAAP or IFRS.

SAB 121 requires a reporting entity that performs crypto asset custodial activities, whether directly or through an agent acting on its behalf, to record a liability with a corresponding asset. It also requires disclosure of the nature and amount of crypto assets the reporting entity is responsible for safeguarding for its customers.

SEC registrants are expected to comply with the guidance in the first interim or annual financial statements ending after June 15, 2022 (e.g., Q2 2022 for calendar year-end public companies), and apply it retrospectively to the beginning of the year. Certain other specified entities are also in the scope of the new interpretive guidance (see [CA 3.7.1](#) in the Appendix).

Questions have arisen regarding the application of SAB 121, including the scope of the guidance. Through informal conversations with the SEC staff and others, we have formed perspectives on the interpretive guidance. This *In depth* discusses the guidance in SAB 121 and addresses frequently asked questions.

The Appendix includes the guidance that will be added to Sections [CA 3.7](#) and [CA 5.2](#) of PwC's *Crypto assets* guide. The guidance formerly included in [CA 3.1.2](#) has been integrated herein.

## Appendix

### 3.7 Accounting for obligations to safeguard crypto assets

Crypto assets may be held by a custodian for safekeeping on behalf of its customers. Arrangements for holding crypto assets can vary, but generally a contract, or terms and conditions, sets out the nature of the arrangement.

If a reporting entity determines that it has control of the crypto assets, the reporting entity records the crypto assets on its balance sheet based on the classification guidance in [CA 1.2](#). The reporting entity will also reflect a corresponding liability to return the crypto assets, which will need to be assessed to determine whether it contains an embedded derivative under ASC 815, *Derivatives and hedging*.

The determination as to whether a reporting entity controls, and therefore should record an asset and a related liability for crypto assets it holds on behalf of its customers, will require the use of judgment based on the facts and circumstances. In determining whether to reflect crypto assets on- or off-balance sheet, a reporting entity may need to consider the following factors, among others:

- The nature of the rights and obligations of the parties defined under legal or regulatory frameworks, or under the terms of a contract
- The rights of the customers to the crypto assets held on their behalf in the event the custodian files for bankruptcy
- The ability of the customer or custodian to transfer, loan, pledge, or encumber the crypto assets
- The ability of the customer to access the private key or transfer the crypto assets to another wallet at any time
- Which party bears the risk of loss as a result of fraud or theft
- Which party obtains the benefits of price appreciation and the impact of price depreciation
- The degree of segregation of crypto assets held on behalf of customers from crypto assets owned by the custodian
- The evidence of ownership of the crypto assets that are held on behalf of the customers (e.g., is the crypto in a separately named wallet or are there off-chain transaction records)

Following this evaluation, if a reporting entity determines it does not have control of the crypto assets, a reporting entity should evaluate whether it has an obligation to safeguard its customers' crypto assets under SAB 121.

#### 3.7.1 SAB 121: scope

##### ***New guidance***

In March 2022, the SEC staff released Staff Accounting Bulletin No. 121 (SAB 121), which addresses the accounting by a reporting entity that engages in activities in which it has an obligation to safeguard crypto assets held for its customers. SAB 121 requires a reporting entity that performs

custodial activities, whether directly or through an agent acting on its behalf, to record a safeguarding liability and a corresponding asset at fair value.

Before applying SAB 121, we believe a reporting entity must first determine whether it has control of the crypto assets (see [CA 3.7](#)). A reporting entity that has control of crypto assets would not be in the scope of SAB 121 and would not record a crypto asset safeguarding obligation to safeguard its own crypto assets.

SAB 121 applies to reporting entities that safeguard their customers' crypto assets either directly or through the use of an agent (i.e., a sub-custodian). To illustrate the application of the guidance, SAB 121 provides an example involving a reporting entity operating a platform that allows users to transact in crypto assets. A "platform" is not a defined term and is not required for reporting entities to be in scope of the guidance.

We believe the following factors, among others, should be considered in assessing whether a reporting entity has an obligation either directly or through an agent acting on its behalf to safeguard a customer's crypto assets (not all factors are required, nor is any one factor determinative):

- *Business model:* Does the reporting entity describe its business model as one of safeguarding customers' crypto assets?
- *Customer relationship:*
  - Do the reporting entity's customers access information about their crypto assets through the reporting entity's platform, application, or website?
  - Would the customer expect the reporting entity to resolve issues or complaints?
  - Does the reporting entity have a contractual obligation or an obligation implied by customary business practices or published policies to safeguard the assets?
  - Does the reporting entity maintain the record keeping and statements that detail the customer's crypto assets?
- *Contractual terms with the customer:* Do the reporting entity's customers know that the reporting entity is utilizing a sub-custodian or are the terms and conditions silent regarding the use of sub-custodians (i.e., would the customer view the reporting entity as responsible for safeguarding the crypto assets)?
- *Contractual terms with the sub-custodian:* Is the account with the sub-custodian an omnibus wallet (which would indicate that the reporting entity is responsible for tracking crypto assets at the individual customer level) or segregated and set up at the individual customer level?
- *Cryptographic key information:* Does the reporting entity maintain cryptographic key information?

The analysis of whether SAB 121 applies should be performed on an entity by entity basis. As a result, more than one entity may be in scope related to custodial services of the same end customer's crypto assets.

Example CA 3-1 illustrates a scenario in which multiple entities would apply SAB 121.

## EXAMPLE CA 3-1

### Platform operator agreement with customers is silent on sub-custodian services

Company A provides its customers with a platform to transact in crypto assets and provides safeguarding services. In order to use the platform, customers sign a contractual agreement with Company A. The agreement is silent as to whether Company A uses a sub-custodian to safeguard the customers' crypto assets, and customers interact directly with Company A for any issues or complaints. Company A enters into an agreement with Company B to provide sub-custodial services and opens an account with Company B in its name for the benefit of its customers. Company B does not have any information about Company A's customers.

Does SAB 121 apply to Company A? Does SAB 121 apply to Company B?

#### *Analysis*

Yes, we believe that both Company A and Company B should recognize a SAB 121 safeguarding obligation and corresponding asset. Although Company A contracts with Company B as a sub-custodian to safeguard its customers' crypto assets, Company A still needs to evaluate whether it is in the scope of SAB 121. Company A owns the relationship with its customers on the platform, and customers interact directly with Company A for any issues or complaints. The customers are not aware that Company B is performing sub-custodial services for Company A. Moreover, Company A's account with Company B is an omnibus account in Company A's name and is not segregated by customer. Based on the foregoing considerations, Company A would likely conclude it is in the scope of SAB 121 and should recognize a safeguarding liability and a corresponding asset.

In addition, Company B should also assess whether it is in the scope of SAB 121. Company A is Company B's customer for sub-custodial services related to crypto assets; therefore, Company B should also recognize a safeguarding liability and a corresponding asset.

---

Question CA 3-1, Question CA 3-2, and Question CA 3-3 address the applicability of SAB 121 based on the type of filing, type of asset, and type of arrangement, respectively.

---

## QUESTION CA 3-1

*Is SAB 121 applicable to all reporting entities?*

---

#### *PwC response*

No. SAB 121 states that the interpretive guidance applies to:

- entities that file reports pursuant to Sections 13(a) or 15(d) of the Securities Exchange Act of 1934 ("Exchange Act") (i.e., existing SEC registrants);
- 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 submitting or filing an offering statement or post-qualification amendment 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 (SPAC).

Additionally, given historical practice of application of SAB Topics, we believe SAB 121 applies to:

- financial statements filed with the SEC under Regulation S-X Rule 3-05, *Financial statements of businesses acquired or to be acquired*; and
- financial statements filed with the SEC under Regulation S-X Rule 3-09, *Separate financial statements of subsidiaries not consolidated and 50 percent or less owned persons*.

Although SAB 121 is not required to be applied by private companies that do not meet any of the circumstances above, we encourage such private companies to consider whether they expect to meet any of these circumstances in the future. Private companies under US GAAP may elect to apply the guidance in SAB 121 voluntarily, and if so, should comply with all of the SEC’s requirements set forth in SAB 121.

### QUESTION CA 3-2

*How are “crypto assets” defined for purposes of applying SAB 121?*

#### **PwC response**

A “crypto asset” is defined in SAB 121 as “a digital asset that is issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques.” Accordingly, in addition to cryptocurrencies (e.g., bitcoin, ethereum), we believe SAB 121 applies more broadly to other crypto assets, including stablecoins, utility tokens, and non-fungible tokens (NFTs).

### QUESTION CA 3-3

*Should a reporting entity that provides custodial services related to assets other than crypto assets similarly apply SAB 121?*

#### **PwC response**

No. SAB 121 should not be applied by analogy to assets other than crypto assets that are safeguarded by a custodian. The SEC staff believes the custodial risks related to crypto assets are different from those of other custodial relationships. These risks include increased regulatory risks as a result of a limited regulatory environment over holding these assets, technological risks (e.g., safeguarding the crypto assets), and the lack of legal precedent due to the unique characteristics of these assets.

## 3.7.2 SAB 121: recognition and measurement

SAB 121 requires a reporting entity that performs custodial activities, either directly or through an agent acting on its behalf, to record a safeguarding liability and a corresponding asset. As there are unique regulatory and legal uncertainties with custodial activities related crypto assets, SAB 121 states that the safeguarding liability should be measured at the fair value of the crypto assets safeguarded by the reporting entity for its customers, and should be remeasured to fair value at each subsequent reporting date. Fair value has the meaning as defined in ASC 820, *Fair Value Measurements*.

Similarly, the corresponding asset should be measured at the fair value of the crypto assets safeguarded by the reporting entity for its customers and remeasured to fair value at each subsequent reporting date (i.e., measured on the same basis as the safeguarding liability). The nature of the corresponding asset is similar to an indemnification asset as described in ASC 805, *Business combinations*. Therefore, like an indemnification asset, a reporting entity would need to evaluate whether any potential loss events, such as theft, impact the measurement of the asset. In practice, we believe the corresponding asset will generally be measured at the same amount as the safeguarding liability unless there is a hack or other event that results in the destruction, loss, or theft of the crypto assets.

We believe the determination of the principal or most advantageous market (as discussed in ASC 820-10-35-5 through ASC 820-10-35-6C) should be the same for the recognition and remeasurement of the safeguarding liability and corresponding asset. See [FV 4.2.2](#) for additional information.

## 3.7.3 SAB 121: derecognition

A reporting entity will need to evaluate when to derecognize a safeguarding liability previously recorded for custodial services of crypto assets. Generally, the safeguarding liability should be derecognized only when the reporting entity no longer has an obligation to safeguard the crypto assets. In many cases this may be straightforward; for example, a reporting entity would derecognize the safeguarding liability at the point in time when a customer is provided with the crypto assets that were safeguarded by the custodian.

For the corresponding asset, derecognition is likely to occur when the safeguarding obligation is relieved and derecognized (e.g., when the customer is provided with the crypto assets that were safeguarded by the custodian). However, in the event of destruction, loss, or theft, derecognition of the corresponding asset may occur sooner than the safeguarding liability.

## 3.7.4 SAB 121: other considerations

### ***Insurance recoveries***

A reporting entity may need to apply additional judgment when there is a loss event and the reporting entity purchased an insurance arrangement to cover the loss of crypto assets. We believe purchasing insurance rarely changes the primary obligation of the reporting entity in an event of loss and is not sufficient to derecognize the safeguarding obligation. Instead, a reporting entity should continue to recognize and measure the safeguarding obligation and separately account for the impact of the insurance policy (which should be accounted for separately from the corresponding asset). Refer to [PPE 8.2.1](#) for guidance on recognition of insurance recoveries. The safeguarding

liability would be derecognized when the obligation is relieved or the reporting entity is legally released from any claims or potential future claims.

### 3.7.5 SAB 121: effective date and transition

SEC registrants are expected to comply with SAB 121 in the first interim or annual financial statements ending after June 15, 2022 (e.g., Q2 2022 for calendar year-end public companies). Such guidance is required to be applied retrospectively to the beginning of the fiscal year in which the interim or annual period relates (e.g., January 1, 2022 for calendar year-end public companies).

SAB 121 also applies to other entities, including but not limited to entities conducting an initial public offering and private operating companies entering into a business combination transaction with a shell company, including SPACs. Such guidance is required beginning with these entities' next submission or filing with the SEC with retrospective application as of the beginning of the most recent annual period ending before June 15, 2022 if the filing includes a subsequent interim period that reflects application of SAB 121. Alternatively, if the filing does not include a subsequent interim period that reflects application of SAB 121, then entities must apply the guidance retrospectively to the beginning of the two most recent annual periods ending before June 15, 2022.

SAB 121 requires transparent disclosure of the effects of the initial application of SAB 121 based on ASC 250-10-50-1 through ASC 250-10-50-3. Disclosures would include the nature and reason for the change. We generally would not expect disclosures to be required related to an impact to the income statement or net assets when the safeguarding liability and corresponding asset are recognized and measured at the same time and at the same amount.

Reporting entities should consider including disclosures required by SAB 74, *Disclosure of the Impact That Recently Issued Accounting Standards Will Have on the Financial Statements of the Registrant When Adopted in a Future Period*, in periods prior to adoption. SAB 74 disclosures would include:

- A brief description of the guidance, the adoption date, and the method of adoption
- The impact of adoption unless not known or reasonably estimable. In that case, a statement to that effect may be made.

Disclosure of other potential impacts is also encouraged (e.g., violations of debt covenants).

See [ESP 30.11](#) for additional information on SAB 74 disclosures.

---

## 5.2 SAB 121: presentation and disclosure

SAB 121 requires disclosures in the footnotes and elsewhere in the filing to address the nature and amount of crypto assets the reporting entity is responsible for safeguarding for its platform users. The disclosures should be disaggregated to disclose each significant crypto asset, including any vulnerability due to concentrations in accordance with ASC 275-10-50. See [ESP 24.3.4](#) for additional information.



In accordance with ASC 235-10-50, the accounting for the crypto asset safeguarding liability and corresponding asset should also be described in the footnotes to the financial statements. See [FSP 1.1.4](#) for additional information.

The reporting entity should also consider disclosure of which party is responsible for recordkeeping and safeguarding the crypto assets, as well as the entity that holds the cryptographic key information. Such entities may include the reporting entity, its agent, or another third party depending on the custodial arrangements.

Given that the crypto asset safeguarding liability and corresponding asset are measured at fair value and remeasured to fair value each reporting period, reporting entities will also need to include the disclosures required by ASC 820.

Question CA 3-4 and Question CA 3-5 address presentation considerations associated with the balance sheet and statement of cash flows, respectively.

---

#### **QUESTION CA 3-4**

*How should the crypto asset safeguarding liability and corresponding asset be classified on a reporting entity's balance sheet?*

---

#### **PwC response**

It depends. We believe the nature of the relationship between the customer and the reporting entity is generally such that the customer has the ability to request withdrawal of the crypto assets and thus terminate the crypto asset safeguarding liability at any time. Accordingly, we believe this on-demand, short-term nature requires the reporting entity to classify both the safeguarding liability and corresponding asset as current on its balance sheet. This is consistent with the guidance on presenting a classified balance sheet in ASC 210. See [FSP 2.3.4](#) for additional information.

---

#### **QUESTION CA 3-5**

*How should the initial recognition and subsequent remeasurement of the crypto asset safeguarding liability and corresponding asset be presented within the statement of cash flows?*

---

#### **PwC response**

ASC 230-10-05-2(c) requires noncash investing and financing activities to be disclosed in the statement of cash flows. As the balance sheet classification of the crypto asset safeguarding liability and corresponding asset is current (see Question CA 3-4) and of an operating nature, the reporting entity would not need to disclose the noncash activity of the initial recognition or subsequent changes in the crypto asset safeguarding liability and corresponding asset. Furthermore, given the general statement of cash flow guidance in ASC 230 provides limited guidance on applying the indirect method and SAB 121 does not address statement of cash flow presentation, we believe a single-line presentation in the reconciliation to net income (i.e., the net effect of revaluing the safeguarding liability and the corresponding asset) would be acceptable.



**To have a deeper discussion, contact:**

**Elizabeth Paul**

*Partner*

Email: [elizabeth.paul@pwc.com](mailto:elizabeth.paul@pwc.com)

**Reto Micheluzzi**

*Partner*

Email: [reto.micheluzzi@pwc.com](mailto:reto.micheluzzi@pwc.com)

**Ryan Blacker**

*Director*

Email: [ryan.w.blacker@pwc.com](mailto:ryan.w.blacker@pwc.com)

*For more PwC accounting and reporting content, visit us at [viewpoint.pwc.com](http://viewpoint.pwc.com). On the go? Take our podcast series with you at the [Viewpoint podcasts page](#).*

© 2022 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.