HOT TOPIC

Digital assets

SEC staff guidance on digital asset safeguarding obligations

April 2022 (updated June 2024)

This Hot Topic summarizes and addresses questions about applying SEC Staff Accounting Bulletin (SAB) No. 121.

On March 31, 2022, the US Securities and Exchange Commission (SEC) published SEC Staff Accounting Bulletin (SAB) No. 121. SAB 121, which added Section FF to SAB Topic 5, reflects SEC staff interpretive guidance about how entities (see Applicability) should account for an obligation to 'safeguard' digital assets. It also outlines disclosures the SEC staff expects entities with these obligations to provide in their SEC filings.

Since the SAB's issuance, questions have arisen, and continue to arise, as preparers, practitioners and other stakeholders apply it. This Hot Topic provides our views, informed in part by consultations and other informal discussions with the SEC staff, about many of those practice questions.

The SAB is now more than two years old. Despite this, new scenarios potentially subject to the SAB continue to emerge and practice continues to evolve around its application. Because of this, our views may continue to evolve and we will likely continue to develop guidance about additional questions not yet addressed herein. We will continue to provide future updates to address those developments as they occur. Given the judgment frequently involved in applying the SAB, we encourage entities to discuss their specific facts and circumstances with their auditors and accounting advisors.

Applicability

SAB 121 applies to financial statements prepared under either US GAAP or IFRS® Accounting Standards:

- by existing SEC registrants;
- by entities that have submitted or filed a not-yet-effective registration statement;
- by entities submitting or filing an offering statement or post-qualification amendment thereto under Regulation A;
- by entities subject to the periodic and the current reporting requirements of Regulation A;
- pursuant to Rules 3-05 and 3-09 of SEC Regulation S-X; and
- by 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).

In a snapshot

SAB 121 creates new asset and liability recognition requirements for entities that have an obligation to 'safeguard' digital assets for others.

Recognition and measurement

An entity's accounting under SAB 121 related to digital assets it holds or otherwise 'safeguards' for others depends on the answer to the following question.

Does the entity 'control' and, therefore, own for accounting purposes the digital assets legally owned by another entity or individual? (see KPMG Hot Topic, *Evaluating custody of digital assets*)?	
Yes	The entity recognizes: • the digital assets; and • a liability to return those assets. The entity's obligation to return the digital assets in the future is evaluated under Topic 815 to determine whether it is, or includes, a derivative (see guidance in KPMG Handbook, Derivatives and hedging).
No	The entity recognizes the following under the SAB (see Question 20): [SAB 121 (Q1)] • a liability for its obligation to safeguard those digital assets ('safeguarding obligation liability'), reflective of the unique risks and uncertainties present in these arrangements; and • a corresponding 'safeguarding asset'. The safeguarding obligation liability is measured initially and subsequently at the Topic 820 fair value of the safeguarded digital assets. The safeguarding asset is measured in the same manner, except that its carrying amount reflects any actual or potential safeguarding loss events, such as resulting from fraud or theft (including hacks). [SAB 121 (Q1, fn 9)]

Disclosures

SAB 121 outlines the following minimum financial statement disclosures the SEC staff expects an entity with digital asset safeguarding obligations to provide: [SAB 121 (Q2)]

- how the issuer is accounting for the safeguarding liability and asset and the effects of initially applying the SAB (see Transition disclosures);
- nature and amount of each significant digital asset that the entity is responsible for safeguarding for others;
- vulnerabilities that the entity has from any concentration of digital asset safeguarding activities;
- required fair value measurement disclosures under Topic 820 related to measuring the safeguarding obligation liability and related asset (subject to adjustment for losses and potential losses) at fair value; and
- who (e.g. the entity, its agent or another third party) holds the cryptographic keys (which may not be a single individual or entity – see Question 120), maintains the internal recordkeeping of those assets, and is obligated to secure the assets and protect them from loss or theft.

Disclosures about significant risks and uncertainties associated with the entity's safeguarding of digital assets for others may also be required both within and outside the financial statements (e.g. in MD&A, risk factors or business description). Examples in the SAB include: [SAB 121 (Q2)]

- types of losses that could occur (e.g. discontinuation or reduction of service usage by customers, litigation, reputational damage, regulatory enforcement actions);
- analysis of the legal ownership of the safeguarded digital assets, including disposition of those assets in the event of the entity's bankruptcy or conservatorship;
- potential effects (financial and otherwise) from destruction, loss, theft, compromise or unavailability of cryptographic keys; and
- information about risk-mitigation steps the entity has in place, such as insurance coverage specifically for digital asset losses.

Effective date and transition

After its issuance in March 2022, existing registrants were required to apply SAB 121 to financial statements for interim and annual periods ending after June 15, 2022, with retrospective application, at a minimum, to the beginning of the fiscal year. [SAB 121 (Q3)]

Other entities subject to SAB 121 when it was issued were required to apply it in their next submission or filing, even if that is imminent. Retrospective application is required to either: [SAB 121 (Q3)]

- the beginning of the most recent annual period ending before June 15, 2022 if a subsequent interim period is presented; or
- the beginning of the two most recent annual periods ending before June 15, 2022 if a subsequent interim period is not presented.

An entity that was not subject to SAB 121 when it was issued may become subject to the SAB later. In such cases, we believe an entity applies the SAB in its first set of financial statements subject to SEC reporting requirements, with retrospective application to either:

- the beginning of the most recent annual period presented (e.g. calendar 2023) if a subsequent interim period (e.g. first quarter 2024) is presented; or
- the beginning of the two most recent annual periods presented if a subsequent interim period is *not* presented (e.g. calendar 2022, if 2022 and 2023 are presented and first quarter 2024 is *not* presented).

Transition disclosures

The SAB stipulates that entities "should include clear disclosure of the effects of the initial application of this guidance," with direction for entities to consult:

- paragraphs 250-10-50-1 – 50-3 (entities applying US GAAP) or IAS 8 (entities following IFRS Accounting Standards) on changes in accounting principle; and
- the supplementary financial information guidance in Item 302 of SEC Regulation S-K. [SAB 121 (Q3, fn 15)]

Topic 250, in general, requires disclosure in the entity's interim and annual periods of adoption of: [250-10-50-1 – 50-2]

- the nature of and reason for the change;
- amounts (e.g. new safeguarding obligation liabilities and assets) recognized on adoption;
- financial statement effects of the change (direct and indirect); and
- prior-period adjustments made (if any).

Questions and answers

The SAB 121 application questions and answers in this section reflect those we have encountered in practice since its issuance. New Questions and Examples added in May and June 2024 are identified with **. Questions that have been substantively updated or revised in May or June 2024 are identified with #.

For purposes of this section, we use and define certain terms as follows.

Term used	Application in this Hot Topic
Digital asset	Any asset that is issued and transferred using distributed ledger or blockchain technology [SEC 'Framework for "Investment Contract" Analysis of Digital Assets' (fn 2)]
Custodian	The entity, whether or not legally a custodian, that may have a safeguarding obligation over a digital asset.
Digital asset owner	The legal owner of the custodied digital asset. As outlined in Question 20, the legal owner of a digital asset might not be its accounting owner; the custodian may 'control' (and therefore, from an accounting perspective, 'own') the digital asset.
Sub-custodian	An entity engaged by a 'custodian' to provide digital asset custodial (safeguarding) services on the custodian's behalf.

Question 10

Does 'crypto-asset' in SAB 121 include stablecoins, CBDCs and NFTs?

Background: See section 2.2.20 of KPMG Issues In-Depth, Crypto intangible assets, for background on stablecoins and central bank digital currencies (CBDCs).

Non-fungible tokens (NFTs) are digital assets that are not interchangeable with other digital assets. This differentiates them from fungible digital assets such as bitcoin and ether, where each bitcoin or ether token is fungible with any other bitcoin or ether token, respectively.

Interpretive response: Yes. SAB 121 uses the term 'crypto-asset' throughout. Its footnote 3 defines 'crypto-asset' as "a digital asset that is issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques." Therefore, 'crypto-asset' is a broader term than 'crypto asset' used in Question 1 of the AICPA Practice Aid, Accounting for and auditing of digital assets (the AICPA Guide).

Based on the definition of 'crypto-asset' used in SAB 121 (including its consistency with the SEC definition of 'digital asset' included above), we believe 'crypto-asset' encompasses, in general, all 'digital assets', including each of the digital asset types in this question, as well as crypto intangible assets like bitcoin, ether and litecoin. [SAB 121 (fn 3)]

Question 15

Can a safeguarding obligation arise for digital assets on a private, permissioned blockchain?

Background: The most widely known blockchains (e.g. Bitcoin, Ethereum) are public, permissionless blockchains. This means, in general, they are decentralized, and anyone can access them. By contrast, access to a private blockchain is limited to invited parties; 'permissioned' refers to different participants having different access or action rights on the blockchain.

On a private, permissioned blockchain, the ability to amend, correct or cancel transactions may exist. For example, a 'master node' may be able to override or countermand an errored or fraudulent transaction.

Question 1 in Appendix B of the AICPA Guide states that digital assets on private, permissioned blockchains where this amend, cancel or correct ability exists ***may*** not exhibit the technological, legal and regulatory risks outlined in SAB 121. [emphasis added]

Interpretive response: Consistent with the 'may' language in Appendix B, Question 1 of the AICPA Guide, we believe it depends on the facts and circumstances. We generally do not believe entities should assume that a safeguarding obligation *cannot* exist over digital assets on a private, permissioned blockchain even if the ability to amend, correct or cancel transactions exists.

While all relevant facts and circumstances should be considered, we believe one important question may be whether there are controls in place to either: (1) prevent a bad actor from realizing the economic benefits from its malfeasance – e.g. selling or exchanging a stolen digital asset for fiat currency, or (2) assure corrective action occurs *before* those economic benefits can be realized. For example, if a bad actor steals a digital asset that resides on the private, permissioned blockchain, are there controls in place that will prevent them from converting that digital asset to fiat currency (or a generally untraceable digital asset like bitcoin) before the fraudulent theft transaction is discovered and can be cancelled?

- If not, that *may* be supportive (albeit, not determinative) to concluding a safeguarding obligation over digital assets on that blockchain does not exist.
- If so, the amend, cancel or correct ability may not substantively mitigate the risks outlined in the SAB; therefore, a safeguarding obligation may exist despite the private, permissioned nature of the blockchain.

Given the judgment involved, we believe entities evaluating whether a SAB 121 safeguarding obligation exists in a private, permissioned blockchain scenario should consult their auditors or other accounting advisors about their specific facts and circumstances.

Question 20

Does SAB 121 apply to the custodian if it is the accounting owner of (i.e. 'controls') the digital asset(s)?

Interpretive response: No. If the custodian 'controls' the digital asset itself, consistent with Question 10 of the AICPA Guide, the custodian records (1) the digital asset as its own asset and (2) a liability to return the digital asset in its financial statements, instead of the safeguarding obligation liability and related asset envisioned by SAB 121. As the accounting owner of the digital asset, the custodian does not have a safeguarding obligation over its own asset.

The preceding paragraph notwithstanding, custodians that determine they control others' digital assets should be mindful of the SEC staff's disclosure expectations set out in the SAB (see In a snapshot). We believe the SEC staff expects them to provide similar disclosures.

KPMG Hot Topic, Evaluating custody of digital assets, provides additional guidance on determining whether the digital asset owner or the custodian, is the *accounting* owner of (i.e. controls) digital assets. The Hot Topic also highlights that the custodian's obligation to return that asset to the digital asset owner in the future needs to be evaluated under Topic 815 to determine whether it is, or includes, a derivative (see KPMG Handbook, Derivatives and hedging).

Question 30#

If the custodian is the accounting owner of the digital asset, will the measurement of the digital asset and digital asset return liability generally be equal like the measurement of the safeguarding obligation liability and safeguarding asset envisioned by SAB 121?

Background: See Question 20.

Interpretive response: Typically, no. Under US GAAP, many digital asset return liabilities are, in effect, measured at fair value (either considering both the return liability and the bifurcated embedded, mark-to-market derivative, or because certain digital asset return liabilities may be financial liabilities in their entirety to which the fair value measurement option under Topic 825 may be applied). [825-10-15-4]

By contrast, the digital asset is *not* measured at fair value (i.e. at least until the adoption of ASU 2023-08, *Accounting for and Disclosure of Crypto Assets*, after which digital assets in scope of Subtopic 350-60 will be measured at fair value – see sections 2.2.10 and 4.2 of KPMG Issues In-Depth, Crypto intangible assets), creating a mismatch between the carrying amounts of the digital asset and the digital asset return liability.

It is not appropriate to measure the recorded digital asset at fair value by analogy to the SAB 121 measurement guidance for safeguarding assets.

Question 40

Is a custodian required to recognize a SAB 121 safeguarding obligation liability if contract provisions limit its liability for adverse digital asset events?

Background: Some contractual arrangements include provisions limiting or expressly disclaiming the custodian's liability for adverse digital asset events such as fraud or theft (hacks).

Interpretive response: Yes. We believe the SEC staff generally intends for entities to record a safeguarding obligation liability (and related asset) under SAB 121 if they are undertaking digital asset custodial or safeguarding activities that carry at least some of the risks (i.e. technological, legal and regulatory) described in the SAB (see Question 50) *regardless* of any contract provisions intended, or that appear, to mitigate some, or even all, of those risks or disclaim any safeguarding obligation. And in a similar manner to identifying implied performance obligations under Topic 606 (revenue from contracts with customers), we believe entities should consider implied risks associated with their digital asset activities – e.g. those implied by the entity's business practices or published marketing or policy material. [606-10-25-16]

At least in part, this appears to be influenced by the staff's view, expressed in the SAB, that "there are significant legal questions around how such arrangements would be treated in a court proceeding arising from an adverse event (e.g., fraud, loss, theft, or bankruptcy)." [SAB 121 (Topic 5 intro)]

Question 50#

Do digital asset custodial (safeguarding) activities need to carry all the types of risks enumerated in SAB 121 to give rise to a 'safeguarding obligation'?

Interpretive response: No. In general, we believe SAB 121 was intended to cast a 'wide net' such that an entity's digital asset custodial (safeguarding) activities do not need to carry all the types of risks (i.e. technological, legal and regulatory) listed in SAB 121 to give rise to a safeguarding obligation under the SAB. Further, the enumerated types of risks were not intended to be an exhaustive list; therefore, entities should also consider whether their activities give rise to other types of risks or uncertainties that may be unique to those activities before reaching a conclusion that they do not have a safeguarding obligation under the SAB.

Question 55**

Can an entity sufficiently mitigate the risks of digital asset custodial (safeguarding) activities such that no safeguarding obligation liability is required?

Interpretive response: Yes, it is possible for an entity to do so. We are aware that the SEC staff have not objected, in at least one specific set of facts and circumstances to date, to a conclusion that a digital asset custodian, despite holding all of the private key information related to the digital wallets holding customers' digital assets, did not need to record a safeguarding obligation liability (and related asset) because the technological, legal and regulatory risks enumerated in SAB 121 were sufficiently mitigated. Those facts and circumstances included all of the following.

- The entity, a regulated financial institution, obtained regulatory approval from its state-level regulator regarding its digital asset custodial activities. Such approval included regulatory review of the entity's risk management and governance practices surrounding those activities. Additionally, the entity appropriately consulted with its relevant federal regulators. The entity observed that its systems and processes relevant to its digital asset custodial activities are subject to continuous supervision and review by its state and federal regulators.
- The entity holds custodial customers' digital assets in a "bankruptcy remote" manner – i.e. those assets would not be available to creditors of the entity in the event of its insolvency or FDIC receivership. This included that:
  - individual, segregated digital wallets are used for each custodial customer;
  - the custodial agreement prohibits the entity from using, including rehypothecating, custodied digital assets; and
  - the custodial agreement includes specific requirements to hold and transfer the digital assets in accordance with customers' instructions.
- The entity obtained a legal opinion from qualified external legal counsel supporting the entity's conclusion that its custodial customers' digital assets would not be available to creditors of the entity in the event of its insolvency or FDIC receivership.

- The entity's contracts with custodial customers clearly established the entity's requisite standard of care and limited scope of liability for blockchain risks outside of its control.
- The entity has comprehensive operational controls in place over private key management that are subject to regular oversight by the entity's regulators.
- The entity has a robust vetting process to assess specific technological, regulatory and/or legal risks for each digital asset it undertakes to custody for customers.

Different facts and circumstances from those described above, even if seemingly similar, may result in a different conclusion; therefore, entities should consult their auditors or other accounting advisors, and potentially the SEC staff and other regulators (if applicable), about their specific facts and circumstances.

Question 60

Are digital asset safeguarding obligations outside the scope of SAB 121 if the custodian does not operate a digital asset trading 'platform'?

Background: The 'Facts' provided in SAB 121 refer to Entity A 'operating a platform that allows its users to transact in crypto-assets'. 'Platform' is not defined in the SAB; nor is it defined in US GAAP, IFRS Accounting Standards or the AICPA Guide.

Therefore, the question arises about whether there are digital asset custodial or safeguarding activities outside the scope of the SAB (that, therefore, could not give rise to a safeguarding obligation) because those activities do not include operating a digital asset trading platform on which users can trade (i.e. buy or sell) digital assets.

Interpretive response: No. We believe it is *not* necessary for an entity to undertake all (or even most) of the business and operating activities ascribed to Entity A in SAB 121. Rather, SAB 121 is intended to apply to any entity undertaking digital asset custodial (safeguarding) activities that carry at least some of the risks (i.e. technological, legal and regulatory) described in the SAB or similar risks (see Question 50), regardless of what other activities the entity does or does not undertake. Entity A's activities are illustrative, rather than a checklist of activities an entity must perform to be in the scope of the SAB.

Question 70

Are digital asset safeguarding obligations outside the scope of SAB 121 if the digital asset owner is not a 'platform user'?

Background: The SAB refers to 'obligations to safeguard crypto-assets held for platform users'. Since the SAB's issuance, questions have arisen about whether the specificity of the reference to 'platform users' indicates an intent by the SEC staff to exclude from the SAB's scope digital asset safeguarding obligations of: [SAB 121 (Summary, Q1)]

- entities that do not operate a 'platform' (see Question 60); or
- digital asset owners that are not 'platform users' (e.g. digital asset owners that do not trade digital assets on the entity's platform, but solely engage the entity for custodial services).

Interpretive response: No. We believe it is not necessary for the digital asset owner to trade digital assets on the entity's platform for a safeguarding obligation to exist.

See Question 40 and Question 50 for additional discussion about what gives rise to a safeguarding obligation under the SAB.

Question 80#

Does SAB 121 apply to broker-dealers subject to Topic 940?

Interpretive response: Yes. Since the issuance of the SAB, numerous interactions with the SEC staff have clarified that broker-dealers are subject to SAB 121 (i.e. broker-dealers are not outside the scope of the SAB). However, as with all other entities, the specific facts and circumstances will determine whether a broker-dealer has a safeguarding obligation to account for under the SAB.

At a February 20, 2024 meeting between the AICPA Stockbrokerage and Investment Banking Expert Panel and members of the SEC staff from the Office of the Chief Accountant and Division of Trading and Markets, the SEC staff shared details about recent SAB 121 consultations involving broker-dealers. In these consultations, the broker-dealer had customers that invested in or held digital assets, while also having an arrangement with a third-party crypto entity that provided digital asset trade execution and safeguarding services for the broker-dealer's customers. In addition, the broker-dealer (or a related party) provided an interface for its customers to submit/transmit digital asset transaction orders to the third-party crypto entity for fulfillment.

The February meeting highlights identify facts and circumstances the SEC staff stated were present *in those consultations* where the SEC staff did not object to the broker-dealer *not* recording a safeguarding obligation liability. Broker-dealers and other entities with similar types of arrangements may find it useful to consider these meeting highlights when evaluating whether their arrangement(s) do or do not give rise to a safeguarding obligation under SAB 121.

Question 90

Does SAB 121 apply to the digital asset owner?

Interpretive response: No. SAB 121 does *not* apply to the digital asset owner; it does not establish any corresponding or new accounting requirements for those entities.

Digital asset owners will continue to account for either (1) the digital asset or (2) a right to receive the digital asset (which is evaluated under Topic 815 to determine whether it is in its entirety, or includes, a derivative – see KPMG Handbook, Derivatives and hedging). KPMG Hot Topic, Evaluating custody of digital assets, provides guidance on making this determination.

Question 100

Can multiple entities (e.g. a custodian and a sub-custodian) have a safeguarding obligation liability and safeguarding asset related to the same custodied digital assets?

Background: A custodian may provide custodial (safeguarding) services to another custodian (i.e. an entity engaged for custodial (safeguarding) services by the digital asset owner). For example, Digital Asset Owner contracts with Custodian B to hold its digital assets. Custodian B, through its existing relationship with Custodian C, engages Custodian C to actually hold Digital Asset Owner's assets in custody (i.e. as sub-custodian).

In this scenario, the question arises about whether Custodian B *and* Custodian C both recognize a safeguarding obligation liability and related safeguarding asset for the same custodied digital assets held by Custodian C.

Interpretive response: Yes. Using the background example to illustrate, we believe that both entities should recognize a safeguarding obligation liability and a safeguarding asset under SAB 121; Custodian B has a safeguarding obligation to Digital Asset Owner, while Custodian C has a safeguarding obligation to Custodian B.

Question 110#

Does an entity have a safeguarding obligation if it is not providing safeguarding services?

Background: Footnote 4 to SAB 121 states that a service of safeguarding another entity's digital assets is in the scope of the SAB if it is *provided by* the entity (Entity A) "or by an agent acting on Entity A's behalf." [emphasis added] [SAB 121 (fn 4)]

SAB 121 also refers to the "*actions of* Entity A to safeguard the [digital] assets," "Entity A is *responsible for* safeguarding the crypto-assets," and "Entity A also *provides a service* where it will safeguard the…crypto-assets." [emphasis added] [SAB 121 (Topic 5.FF Facts (Q1)]

Question 100 explains that multiple entities can have an obligation to safeguard the same digital assets, while Question 123 observes that an entity can be providing safeguarding services even if it holds no cryptographic key information.

Interpretive response: No. We believe in order for an entity to have a safeguarding obligation under SAB 121 it must be, consistent with the SAB language in the background ('actions', 'responsible for', 'provides a service'), providing (i.e. is a principal to) the safeguarding services, and not merely arranging (i.e. as an agent) for them to be provided by a third party.

The SAB does not provide guidance about how to make this determination. However, we believe it should take into consideration all relevant facts and circumstances, which may include (not exhaustive):

- who owns the customer relationship, and who the digital asset owner would consider (i.e. perceive) to be the party safeguarding its digital assets;
- the terms and conditions of the contract(s) (or similar – e.g. 'terms of service') between (1) the entity and the digital asset owner and (2) the entity and the third party;
- to which entity the digital asset owner goes (or would go) for issues about the acceptability of the safeguarding services (e.g. if it were unable to access or trade its digital assets);
- whether the entity knows the public key for, and digital asset balance(s) in, the account(s) in which the owner's digital assets are held;
- the extent to which the entity has implemented processes to safeguard digital assets;
- the extent to which use of a third party is contemplated by the terms of the contract (or, in the absence of a formal contract, the platform/exchange terms and conditions) between the digital asset owner and the entity;
- which entity – i.e. the entity or the third party – is responsible for account recordkeeping;
- how the digital asset owner accesses the held digital assets (e.g. through the entity or through the third party); and

- the extent and nature of the entity's involvement with transactions involving the digital assets.

In addition, we believe it may often be appropriate to consider factors that frequently weigh into principal versus agent evaluations for service arrangements under Topic 606 (revenue from contracts with customers). The considerations and factors outlined in Question 9.3.60 in KPMG Handbook, Revenue recognition, for determining whether an entity is a principal to providing services when a third party (e.g. a sub-custodian) is involved may be useful.

Question 120#

Does an entity have a safeguarding obligation if it (including its sub-custodians, if any) does not control all the private key information associated with the digital asset wallet?

Background: In some arrangements, the wallet service (or software) provider (or its agents) controls all the private keys associated with the wallet. For example, this is generally the case in an omnibus (i.e. non-segregated) wallet scenario.

However, in other arrangements, the wallet service (or software) provider controls some private key information, but not enough to execute wallet transactions. For example:

- **Scenario 1:** A multi-signature wallet with three private keys may require two of those keys to execute a transaction, and the wallet service provider may hold only one (the digital asset owner holding the other two). Therefore, the wallet service provider can neither (1) move digital assets out of the wallet without the digital asset owner's concurrence, nor (2) block such actions of the digital asset owner.
- **Scenario 2:** A dual-signature wallet may require the digital asset owner and the wallet service provider to both use their private keys to execute a wallet transaction. In this scenario, the wallet service provider cannot move digital assets out of the wallet without the digital asset owner's concurrence but can block such actions by the digital asset owner.
- **Scenario 3:** Under multi-party computation (MPC), multiple parties each hold a portion of the private key (i.e. a key 'shard' or 'share'). A certain number of key shards (e.g. three of five) are necessary to execute a transaction. It may also be the case that one or more specific key shards is required to initiate and/or authorize a transaction from the wallet (e.g. key shard A *must* be engaged along with any two of four remaining key shards B-E).

Since the SAB's issuance, questions have arisen about whether the wallet service (or software) provider in these types of scenarios has a safeguarding obligation under the SAB.

Interpretive response: It depends. We believe a safeguarding obligation exists and must be accounted for under the SAB when the entity *either*:

- controls enough private key information to execute wallet transactions (e.g. if the entity held two of the three private keys in Scenario 1 instead of only one, or has the requisite number of key shards – and, if applicable, the specific key shard(s) needed – to execute transactions in Scenario 3); or
- controls enough private key information to block wallet transactions (i.e. as in Scenario 2).

This is because, from the perspective of the digital asset owner, an inability to move (or retrieve) its digital assets may be as damaging as a theft of those digital assets. Consequently, under either circumstance, we believe the entity has an obligation to safeguard the digital assets for which it has that private key information.

There is no 'one-size-fits-all' answer about whether an entity holding a lesser amount of private key information – i.e. such that it cannot unilaterally execute or block wallet transactions – has a SAB 121 safeguarding obligation. This topic, and new scenarios, continue to be a subject of discussions in practice; therefore, we believe entities in this situation should consult with their auditors or other accounting advisors about their specific facts and circumstances and not assume they do not have a safeguarding obligation under the SAB.

Example 120.1 that follows illustrates one fact pattern. The conclusion reached is based on consideration of all the relevant facts and circumstances. Even relatively minor changes to the underlying facts and circumstances *could* affect the conclusion reached.

Example 120.1**
MPC wallet scenario

ABC Company (ABC) provides software to customers whereby the customer generates and controls the private key information as described in Question 125. *However*, ABC's technology also allows customers to 'shard' the private key created by the software for distribution to different, segregated computers/devices. Customers have the option for ABC to hold one or more key shards, and therefore participate in the authorization and execution of wallet transactions. In these cases, ABC's held key shards are administrative in nature; those key shards automatically (i.e. without ABC personnel intervention) co-sign wallet transactions that must be initiated and approved by *non-ABC held* key shards.

ABC concludes it does not have a SAB 121 safeguarding obligation when it holds customer wallet key shards and participates in the authorization and execution of wallet transactions. In reaching this conclusion, ABC considers all facts and circumstances around these arrangements, including, first, the following related to the wallet's private key information.

- ABC *never* controls enough key shards to block wallet transactions; therefore, the customer never needs ABC's key shards to execute a transaction.
- The customer (and/or third parties it alone engages, in arrangements to which ABC is not a party) *always* maintains the key shards necessary to initiate and execute a wallet transaction; that is, ABC never controls the shard(s) necessary to initiate or unilaterally approve wallet transactions. ABC can only *contribute* to the execution of wallet transactions initiated and approved by the customer via the customer's controlled key shards.
- The customer has sole, unilateral control over the software's policy manager; this means the customer can, at any time, for any reason and without penalty, remove ABC from the transaction authorization process.
- ABC has no ability to restore or replace the private key or shards thereof, nor does it have any ability at any time to access or recreate the seed phrases for the digital wallet used to generate the private key. By contrast, the customer, via its sole possession of the seed phrases, can recreate the private key to the wallet if it is lost.

ABC then further assesses that its generally sophisticated customers would not perceive ABC as safeguarding their digital assets. This assessment is based on the private key information facts above along with the following additional facts and circumstances.

- The terms of service with customers make clear that:
  - customers are solely responsible for their private key information, can recover their own private key without ABC's assistance and do not need ABC to transact in their wallets; and
  - ABC cannot recover (or assist in recovering) private key information (including seed phrases) for customers.

- ABC has no reporting or recordkeeping responsibilities to the customer related to wallets secured using the ABC software.
- ABC has no history of fielding complaints related to wallet access or lost/stolen digital assets; ABC's customer service history is consistent with that of any typical software provider.

Question 123

Can an entity have a safeguarding obligation if it controls or maintains *no* private key information?

Background: Footnote 4 to SAB 121 states that a service of safeguarding another entity's digital assets is in the scope of the SAB if it is provided by the entity (Entity A) "*or by an agent acting on Entity A's behalf.*" [emphasis added] [SAB 121 (fn 4)]

Interpretive response: Yes, if another entity that *does* control some or all of the private key information has a safeguarding obligation and that entity is determined to be an agent (i.e. providing safeguarding services *on behalf*) of the entity. Question 110 outlines considerations for determining whether another entity involved in safeguarding digital assets is an agent of the entity in question.

Question 125

Does an entity that *only* provides wallet software tools have a safeguarding obligation?

Background: Question 5 in Appendix B of the AICPA Guide asks: "If an entity ***only provides wallet software tools*** to a customer whereby ***the customer generates and controls the private key information***, would the entity's transaction with the customer give rise to a safeguarding obligation within the scope of SAB No. 121?" [emphasis added]

It then concludes "No. If the entity ***only provides software tools*** to the customer, ***who then generates and controls the private key information***, the transaction does not give rise to a safeguarding obligation." [emphasis added]

Interpretive response: No. However, an entity should thoroughly evaluate all relevant facts and circumstances around its involvement with the digital asset owner's acquisition and holding of the owner's digital assets to determine (consistent with the emphasized Question 5 text above) (1) whether it 'only' provides wallet software tools and (2) who generates or controls the wallet private key information. Significant judgment may be involved in evaluating these scenarios and determining, based on the facts and circumstances, whether the entity has a safeguarding obligation. Given the nature of these judgments, we recommend that entities consult with their auditors or other accounting advisors about their specific facts and circumstances.

Question 130

How should an entity measure and record any reduction of the safeguarding asset resulting from a loss (or potential loss) event?

Background: SAB 121 states that the entity needs to evaluate whether any potential loss event (e.g. theft) affects the measurement of the safeguarding asset. [SAB 121 (fn 9)]

SAB 121 analogizes the safeguarding asset to an indemnification asset recognized in a business combination under Topic 805 (or IFRS 3). Paragraphs 7.168 – 7.173a in KPMG Handbook, Business combinations, provide additional guidance on the accounting for business combination indemnification assets. [SAB 121 (fn 8)]

Interpretive response: We believe using the loss contingency model in Subtopic 450-20 (loss contingencies) is one acceptable approach to determine whether to reduce the carrying amount of the safeguarding asset for a loss (potential loss) event and, if a reduction is warranted, by what amount. There may be other acceptable approaches.

If a reduction to the carrying amount of the safeguarding asset – i.e. to an amount less than the safeguarding obligation liability – is warranted by a loss (or potential loss) event, we believe the reduction should be recognized as a loss in the current period P&L. The loss, in effect, reflects the expected economic cost to satisfy the safeguarding obligation stemming from the loss (or potential loss) event.

If the expected amount of the loss changes (up or down), we believe such changes should be reflected in the same income statement line item as the original loss, with a corresponding adjustment to the carrying amount of the safeguarding asset.

Insurance recovery

A custodian may have insurance that covers digital asset losses. In general, we believe that an expected insurance recovery receivable should be recognized separately from the related safeguarding asset – i.e. the receivable should not be combined with the safeguarding asset. Insurance recoveries should only be recognized in the P&L to the extent that: [410-30-35-8, 450-20-25-1]

- costs and losses clearly attributable to the insurable event have been incurred and recognized; and
- the recoveries are probable (i.e. likely to occur) and estimable.

This probability approach is commonly referred to as the 'loss recovery model'. Judgment, based on the specific facts and circumstances of the claim, is often required. In some cases, perhaps especially in the context of digital asset claims (e.g. because of the relatively limited body of digital asset case law), it may be difficult to reach the probable threshold until the claim is filed, processed or even settled. Settlement of a claim after the reporting date may indicate that the probable threshold was met at the reporting date. [855-10-25-1]

Insurance recoveries that exceed the costs and losses recognized in earnings are contingent gains. Contingent gains are recognized only when settled. [450-30-25-1]

Question 135

Does an entity need to record a reduction to the safeguarding asset for a loss (or potential loss) event if it is not legally liable to the digital asset owner?

Background: Consider the following scenario.

- Entity A does not control any of the private key information for the digital wallet holding Owner B's digital assets; Custodian C controls all of the private key information.
- Entity A is determined to have a SAB 121 safeguarding obligation consistent with Question 123. It therefore has recorded a safeguarding obligation liability and related safeguarding asset.
- A loss event of the nature contemplated in Question 130 occurs.
- Under the terms of Entity A's arrangement with Custodian C and an appropriately considered legal evaluation, Custodian C is contractually and legally responsible for the safeguarding loss event.

In this scenario, the question arises as to whether Entity A should account for the safeguarding loss event as described in Question 130 – i.e. by reducing the carrying amount of the safeguarding asset, with a corresponding loss in the P&L.

Interpretive response: Yes. While Entity A may not be contractually or legally liable for the safeguarding loss, SAB 121 applies, in effect, a 'constructive' versus legal obligation approach to determining whether an entity has a safeguarding obligation (see Question 40). We believe it would be inconsistent with the conclusion that Entity A has, and must account for, a safeguarding obligation to Owner B for Entity A not to record the effects of the safeguarding loss event. Therefore, we would expect Entity A to record the safeguarding loss event in a manner consistent with that described in Question 130. Entity A would separately consider whether it has, and account for, any right to recover that loss from Custodian C.

This Question assumes that Entity A's conclusion that it is not contractually or legally liable to Owner B is valid; it does not address whether that conclusion is appropriate.

Question 140

How should a custodian classify the safeguarding obligation liability and related safeguarding asset on the balance sheet if the digital asset owner can withdraw its digital assets at any time?

Background: SAB 121 does not provide guidance on how an entity should classify the safeguarding obligation liability and related asset on the balance sheet.

Interpretive response: We believe the safeguarding obligation liability should be classified as a current liability and the safeguarding asset should be classified as a current asset if the digital asset owner can substantively terminate the custodian's safeguarding obligation at any time by withdrawing the custodied digital assets.

Under SEC Regulation S-X, entities should separately present (on the face of the balance sheet or in a note to the financial statements): [Reg S-X Rule 5-02]

- a current safeguarding obligation liability if it exceeds 5% of total current liabilities; and
- a current safeguarding asset if it exceeds 5% of total current assets.

Question 150

When should an entity derecognize its safeguarding obligation liability?

Interpretive response: We believe that, in general, an entity would not derecognize its safeguarding obligation liability until the custodied digital assets are returned to the digital asset owner (and therefore, the entity is relieved of its safeguarding obligation), or in the case of a claim or potential claim stemming from a loss event, only upon legal release therefrom (or confirmation that there are no further potential claims). [405-20-40-1]

Question 160

How does a SAB 121 digital asset safeguarding obligation liability and corresponding asset affect the entity's statement of cash flows?

Interpretive response: The initial recognition of the safeguarding obligation liability and safeguarding asset is a noncash transaction that we believe is generally operating in nature. Therefore, it is neither presented in the statement of cash flows, nor separately disclosed under Topic 230.

In subsequent periods, we believe it is acceptable to present any difference between the remeasurement of (1) the safeguarding obligation liability and (2) the safeguarding asset during the period – e.g. from a loss (or potential loss) event (see Question 130) – on a net basis. This net difference should be presented as a reconciling item in the reconciliation of net income to net cash flows from operating activities (see section 3.2 of KPMG Handbook, Statement of cash flows).

Question 170**

How does a SAB 121 digital asset safeguarding obligation liability and corresponding asset affect an entity's deferred tax accounting?

Interpretive response: We believe the recognition of safeguarding obligation liabilities and related safeguarding assets requires entities to recognize deferred tax assets and deferred tax liabilities not previously recognized. We further believe that these deferred tax assets and liabilities should be disclosed on a gross basis for reasons generally consistent with why deferred tax assets and liabilities arising from operating lease liabilities and operating lease right-of-use assets are presented on a gross basis (see paragraph 9.082a of KPMG Handbook, Accounting for income taxes).

For further information

See KPMG Executive Summaries & Issues In-Depth, as well as other digital asset Hot Topics.

Contact us

Scott Muir
Partner

smuir@kpmg.com

Michael Hall
Partner

mhhall@kpmg.com

Learn about us: **kpmg.com**