



June 27, 2022

VIA ELECTRONIC SUBMISSION

Paul Munter  
Acting Chief Accountant  
Office of the Chief Accountant  
U.S. Securities and Exchange Commission  
100 F Street, NE  
Washington, DC 20549

**Re: Update on Efforts to Implement Staff Accounting Bulletin No. 121  
“Accounting for Obligations to Safeguard Crypto-Assets an Entity  
Holds for its Platform Users” (“SAB 121”)**

Dear Mr. Munter:

The Securities Industry and Financial Markets Association (“SIFMA”)<sup>1</sup> and the American Bankers Association (“ABA”)<sup>2</sup> appreciated the opportunity to speak with the Securities and Exchange Commission’s (“SEC”) Office of the Chief Accountant (“OCA”) and Division of Corporation Finance (collectively, the “Staff”) on June 3, 2022 regarding SAB 121 and our request to defer its effective date<sup>3</sup>. As discussed, our member firms are working diligently across various functions to bring to the Staff well-developed fact patterns for analysis – whether individually, through the SIFMA and ABA Accounting Committees or through the Association of International Certified Professional Accountants Digital Asset Working Group (“DAWG”) – but this very time-consuming process is on-going.

---

<sup>1</sup> SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry’s nearly one million employees, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. With offices in New York and Washington, D.C., SIFMA is the U.S. regional member of the Global Financial Markets Association (GFMA).

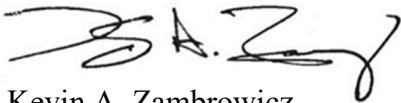
<sup>2</sup> The American Bankers Association is the voice of the nation’s \$24.0 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard \$19.9 trillion in deposits and extend \$11.4 trillion in loans.

<sup>3</sup> Kevin Zambrowicz, SIFMA, and Michael Gullette, ABA, Letter to Paul Munter, Acting Chief Accountant, U.S. Securities and Exchange Commission (May 27, 2022), available at <https://www.sifma.org/wp-content/uploads/2022/05/SAB-121-Deferral-Request-5.27.2022.pdf>.

In advance of providing these specific fact patterns, we have (1) identified various factors specific to banking organizations that we believe sufficiently mitigate the risks outlined in SAB 121, to facilitate immediate discussions with the Staff on how our member firms should evaluate the scope of the guidance given their specific facts and circumstances (*Attachment A*); (2) summarized certain of the specific fact patterns we expect to provide, for the Staff's reference, to articulate the range of matters on which we believe clarity would be helpful, particularly as it relates to the definition of "crypto-assets" (*Attachment B*); and (3) outlined a series of questions regarding the recognition, measurement and disclosure of the safeguarding liability (which are not fact pattern-specific), to help clarify the appropriate application of the guidance in SAB 121 (*Attachment C*).

To the extent the Staff has any questions on these attachments, please do not hesitate to contact Kevin Zambrowicz or Michael Gullette. We thank you again for your willingness to continue the dialogue on these and other issues.

Regards,



Kevin A. Zambrowicz  
Managing Director & Associate General Counsel  
SIFMA



Michael L. Gullette  
Senior Vice President, Tax and Accounting  
ABA

Attachments (3):

*Attachment A*: Factors Specific to Banking Organizations that Address SAB 121 Risks

*Attachment B*: Summarized Fact Patterns Expected to be provided to OCA Staff on a Future Date

***Attachment C: Questions Regarding Recognition, Measurement and Disclosure of the Safeguarding Liability***

CC: Nellie Liang  
Under Secretary for Domestic Finance  
U.S. Department of the Treasury

Benjamin W. McDonough  
Senior Deputy Comptroller and Chief Counsel  
Office of the Comptroller of the Currency

Harrel Pettway  
General Counsel  
Federal Deposit Insurance Corporation

Mark E. Van Der Weide  
General Counsel  
Board of Governors of the Federal Reserve System

## Attachment A<sup>4</sup>

### Factors Specific to Banking Organizations that Address SAB 121 Risks

#### I. Executive Summary

According to SAB 121, 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. In this context, the Staff indicates that 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.** SAB 121 states, “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.** SAB 121 states, “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.** SAB 121 states, “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”.

We believe, however, that these risks are sufficiently mitigated for banking organizations because of the stringent regulatory and supervisory frameworks within which they operate. In the following sections, we describe the existing safeguarding activities performed by our member firms to provide background and context. We then detail the various risk-mitigating factors specific to our member firms. We look forward to engaging with the Staff on these

---

<sup>4</sup> SIFMA, ABA and the Bank Policy Institute (“BPI”) have sent a separate letter to the Department of the Treasury, Federal Deposit Insurance Corporation (“FDIC”), Office of the Comptroller of the Currency (“OCC”) and Board of Governors of the Federal Reserve System (the “FRB”) and, collectively with the OCC and the FDIC, the “Banking Agencies”) that includes an analysis similar to that found in Attachment A (“Banking Agency Letter”). OCA was copied on the Banking Agency Letter.

points in more detail, including our member firms' view that these factors provide an appropriate basis for not recording a safeguarding liability per Question 1 in SAB 121 when safeguarding crypto-assets. In other words, we aim to confirm that the requirements in Question 1 apply to entities that provide the activities described, *only if the aforementioned risks are in fact present*.

## II. Custody and Safekeeping Activities of Banking Organizations

Banking organizations provide safekeeping services to institutional and other investors globally, playing an essential role in ensuring the safety of client assets and the stability of the financial markets. As described at length by the OCC in Interpretive Letter 1170:

Safekeeping services are among the most fundamental and basic services provided by banks. Bank customers traditionally used special deposit and safe deposit boxes for the storage and safekeeping of a variety of physical objects, such as valuable papers, rare coins, and jewelry [...].

Traditional bank custodians frequently offer a range of services in addition to simple safekeeping of assets. For example, a custodian providing core domestic custody services for securities typically settles trades, invests cash balances as directed, collects income, processes corporate actions, prices securities positions, and provides recordkeeping and reporting services [...] OCC guidance has recognized that banks may hold a wide variety of assets as custodians, including assets that are unique and hard to value. These custody activities often include assets that transfer electronically. The OCC generally has not prohibited banks from providing custody services for any particular type of asset, as long as the bank has the capability to hold the asset and the assets are not illegal in the jurisdiction where they will be held.<sup>5</sup>

Today, the majority of custody services are provided to customers through securities accounts and cash accounts maintained by banking organizations.<sup>6</sup> The value-added role played by custodians in the financial system is widely understood and appreciated by both market participants and the regulatory community. Custodians are responsible for safekeeping and segregating customer assets, providing a broad range of related financial services, and

---

<sup>5</sup> OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020) at 6-7 (citations omitted).

<sup>6</sup> The ClearingHouse, The Custody Services of Banks (July 2016) at 3-4, *available at* [https://www.theclearinghouse.org/-/media/tch/documents/research/articles/2016/07/20160728\\_tch\\_white\\_paper\\_the\\_custody\\_services\\_of\\_banks.pdf](https://www.theclearinghouse.org/-/media/tch/documents/research/articles/2016/07/20160728_tch_white_paper_the_custody_services_of_banks.pdf).

establishing relationships with central securities depositories that allow records of ownership of securities to be maintained in book-entry form.<sup>7</sup> Custodial services are offered in a manner that protects client assets from misappropriation or loss and the use of such services is often required by law or regulation.<sup>8</sup> Some custody services may be provided by nonbanks, but clients generally prefer (and in some cases are legally required) to use banking organizations that are subject to robust prudential regulation and oversight, and that can provide access to deposit accounts and payment systems. For example, Section 17(f) of the Investment Company Act of 1940 (the “ICA”)<sup>9</sup>, viewed as the “gold standard” for custody, requires a mutual fund to maintain its securities and similar investments with entities under conditions designed to maintain the safety of fund assets. As a practical matter, most mutual funds place their assets with a bank custodian. Under Rule 206(4)-2 of the Investment Advisers Act of 1940, known as the “custody rule”, registered investment advisers that have custody of client assets must use a “qualified custodian”, including banking organizations, to maintain those assets.<sup>10</sup>

The ability of the OCC, the FDIC and the FRB to appropriately regulate and supervise safekeeping activities is well-recognized. For example, when Congress passed the Gramm-Leach-Bliley Act in 1999, removing the global bank exemption from the definitions of broker and dealer under Sections 3(a)(4) and 3(a)(5) of the Securities Exchange Act of 1934, Congress provided an exception for banks to continue to provide securities-related safekeeping and custody services for their customers without registering as a broker-dealer.<sup>11</sup> This statutory exception expressly recognized that the safekeeping activities conducted by banking organizations do not require additional regulation or other oversight by the market regulator for custody activities (*i.e.*, the SEC through the requirement to register as a broker-dealer).

While banking organizations today generally do not offer crypto-asset custody services at scale, they are involved in many areas of financial innovation involving decentralized ledger technology, including the development of safeguarding solutions for crypto-assets. Banking organizations, subject to comprehensive safety and soundness and prudential regulation, historically have adapted controls and practices to evolve with technology, the financial markets and their customers’ resulting demands, and have provided custody and other services for a range of asset classes, from paper certificates in vaults, to records in computer databases, to tokenized assets.

---

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> 15 U.S.C. § 80a-17(f).

<sup>10</sup> 17 CFR § 275.206(4)-2. Furthermore, the rule imposes certain client notice, account statement and surprise audit mandates.

<sup>11</sup> 15 U.S.C. § 78c(a)(4)(B)(viii).

The OCC has acknowledged that custody services change with markets and technology, stating “[w]hile the use of electronic media to store and access items raises additional risks, banks already have extensive expertise in dealing with these risks and OCC has provided guidance on addressing these risks”.<sup>12</sup> Indeed, banks have been granted authority to safekeep private, encryption keys outside of the context of crypto-assets and have developed appropriate risk management to do so.<sup>13</sup> Specifically, in 1998 the OCC found that “a dual control system of key escrow in which both the client and the [bank subsidiary] would have separate keys needed to be used jointly to recover the escrowed key” sufficiently addressed any risk that “misappropriation of key data could result in harm to a customer”.<sup>14</sup> Bank custodians are therefore well-placed to continue to develop leading risk management approaches for the safekeeping of assets, thereby enhancing efficiencies and reducing risks as various technologies evolve.

Modern custody services have been offered by banking organizations for over 80 years, with significant success. These custodied assets are held safely and are made available to customers, as the types of risks that the SEC cites as being of concern are mitigated effectively through the legal and regulatory frameworks applicable to banking organizations. Their success has instilled confidence in the public in their ability to act as custodian and as of the end of the first quarter of 2022, the largest bank custodians collectively held more than \$200 trillion in assets under custody.<sup>15</sup> Throughout this history, two key principles have remained constant. First, as discussed in further detail below, regulated custodians have been required to properly segregate assets under custody at all times, thereby resulting in assets under custody being treated as property of the client. Second, banking organizations are subject to stringent supervision and regulation, which has led banks to be the custodian of choice for legislators and regulators as they have developed laws and regulations to protect investors in new asset classes.<sup>16</sup> Similar

---

<sup>12</sup> OCC Conditional Approval No. 479 (July 27, 2001).

<sup>13</sup> OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020) (citing OCC Conditional Approval No. 267, granting a national bank authority to safekeep encrypted keys).

<sup>14</sup> OCC Conditional Approval No. 267.

<sup>15</sup> Global Custodians, Custodians by assets under custody and administration, Q1 2022 Rankings, *available at* <https://www.globalcustodian.com/custodians-assets-under-custody/>.

<sup>16</sup> The structure and legislative history of the ICA, which raised a number of concerns about misappropriation of investment company assets in custody, indicates that banks were viewed as appropriate custodians for mutual fund assets as there was no effort to impose specific, additional requirements on bank custodians. *See, e.g.*, 15 U.S.C. 80a-3 (carving out banks and certain funds maintained by banks from the definition of “investment company”); Hearings S. 3580 Before the Subcomm. of the Senate Comm. on Banking and Currency, 76th Cong., 3d Sess. 264 (1940). *See also* 62 Fed. Reg. 26923, 26925 (May 16, 1997) (“the legislative history of [section

principles continue to apply today to the safekeeping of crypto-assets, and the important role of banking organizations in the evolution of the crypto-asset marketplace should be encouraged.

### III. Factors Specific to Banking Organizations that Address the Risks Noted in SAB 121

#### A. **Technological risks**

The technological risks associated with crypto-asset activities are limited for regulated banking organizations because the regulatory and supervisory framework and consistent oversight already applicable to these entities ensure that such risks are appropriately mitigated.

##### 1. **Regulatory and Supervisory Guidance Requiring Mitigation of Technological Risks**

The technological risks noted in SAB 121 are limited by the stringent regulatory oversight of the Banking Agencies over banking organizations' safekeeping activities. For example, banking organizations are expected to "gather assets, effectively employ technology and efficiently process huge volumes of transactions" while minimizing "the potential that events, expected or unexpected, may have an adverse impact on a [banking organization's] capital or earnings."<sup>17</sup>

As a gating matter, OCC Interpretive Letter 1179 requires a banking organization to receive supervisory non-objection regarding risk management systems and controls from the OCC before conducting crypto-asset custody activities under OCC Interpretive Letter 1170.<sup>18</sup> Thus, a banking organization regulated by the OCC would not be permitted to engage in these activities until the OCC is satisfied the relevant risks are addressed. Other U.S. banking regulators and global standard setters apply similar processes and standards.<sup>19</sup> Specific risks

---

17(f) of the ICA] suggests that the section was intended primarily to prevent misappropriation of fund assets by persons having access to assets of the fund".) This legislative history likely reflects the view that the existing regulatory regime for banks would adequately safeguard mutual fund assets.

<sup>17</sup> OCC, *Comptroller's Handbook: Custody Services* (Jan. 2002) at 1, 2. See generally OCC, *Comptroller's Handbook: Asset Management Operations and Controls* (Jan. 2011), OCC, *Comptroller's Handbook: Unique and Hard-to-Value Assets* (Aug. 2012), OCC, *Comptroller's Handbook: Retirement Plan Products and Services* (Feb. 2014), OCC, *Comptroller's Handbook: Conflicts of Interest* (Jan. 2015) and OCC Bulletin 2013– 29, *Third-Party Relationships—Risk Management Guidance* (Oct. 30, 2013).

<sup>18</sup> OCC Interpretive Letter No. 1179, Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank (Nov. 18, 2021); OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020).

<sup>19</sup> FDIC, FIL-16-2022, Notification of Engaging in Crypto-Related Activities (April 7, 2022); BCBS, Consultative Document: Prudential treatment of crypto-asset exposures (June 2021) at 16 ("Banks are also expected to inform



unique to crypto-asset custody highlighted in OCC Interpretive Letter 1170 that banking organizations are required to address include the treatment of “forks” (which must be addressed in the custody agreement), settlement of transactions, physical access controls, security servicing, and specialized audit procedures.<sup>20</sup>

In contrast to nonbank entities, banking organizations are thus uniquely positioned to address risks arising from custody activities because of their existing risk management processes and infrastructure that have been developed over the years to meet stringent regulatory requirements. In fact, the New York State Department of Financial Services, likely due in part to its assessment of the ability of banking organizations to manage risks associated with crypto-asset activities, exempted New York State banks from the requirement to obtain a license to engage in crypto-asset business activities.<sup>21</sup>

## 2. Practices for Crypto-assets Held Under Custody

The technology-related risks that must be managed when providing safekeeping services for crypto-assets include the comingling of assets, risk of loss, risk of theft and risk of information technology (“IT”) failure.<sup>22</sup> Banking organizations manage these risks for other financial assets today by using systems, controls and practices that establish exclusive control over the custodied asset and that are consistent with industry best practices to protect against theft, loss and unauthorized or accidental transactions. These practices and processes would be applied to crypto-assets in the manner described in the following table.

---

their supervisory authorities of their policies and procedures, assessment results, as well as actual and planned crypto-asset exposures or activities in a timely manner and to demonstrate that they have fully assessed the permissibility of such activities, the associated risks and how they have mitigated such risks.”).

<sup>20</sup> *Id.* See also OCC, *Comptroller’s Handbook: Custody Services* (Jan. 2002) (providing detailed guidance on risk management practices and risk management controls for banks providing custody services).

<sup>21</sup> 23 CRR-NY 200.3(c)(1).

<sup>22</sup> In the context of crypto-assets, the risk of commingling of assets is the risk that assets belonging to a client are used by either the custodian or another client to satisfy a financial claim or obligation. The risk of loss is the risk that the asset is lost and that it cannot be retrieved by either the custodian or the client. The risk of theft is the risk that a third-party gains access to the asset and is able to move the asset to a wallet outside of the control of the custodian or client. The risk of IT failure is the risk that the custodian’s systems or controls may fail or otherwise prove inadequate to properly identify and/or protect the client’s assets, including from a cyber incident.

**Table 1: Summary of Practices for Safekeeping Crypto-assets**

<i>Key Principle</i>	<i>Application to Crypto-assets</i>
<p><b>Separation of Custody and Trading Activities</b></p>	<ul style="list-style-type: none"> <li>• To ensure appropriate oversight and control, the banking organizations’ safekeeping function would be functionally separated from the banking organizations’ trading function.</li> </ul>
<p><b>Segregation of Client Assets from Banking Organization Assets</b></p>	<ul style="list-style-type: none"> <li>• As with any other financial asset, banking organizations would ensure the segregation of client assets at all times, and would undertake the daily reconciliation of books and records. This segregation can be achieved in a number of ways, which may differ based on the attributes of a particular crypto-asset.</li> <li>• When combined with an agreement by the custodian and client to treat the asset as a “financial asset” under Uniform Commercial Code (“UCC”) Article 8, the asset generally should be bankruptcy-remote.</li> </ul>
<p><b>Proper Control</b></p>	<ul style="list-style-type: none"> <li>• The management of private key technology is a critical and foundational element to exercising control over the asset. A core risk of this technology is the potential of a “single point of failure” with respect to the key (<i>i.e.</i>, where one event could result in the loss, theft or other misuse of the asset associated with the key).</li> <li>• The technology supporting private keys has advanced significantly in recent years and it is now possible to have private keys that are represented by multiple encrypted “shards”, where no single party can authorize the transfer or disposition of the asset.</li> <li>• To the extent that any one shard is lost or rendered inoperable, the remaining shards can support the retrieval of the asset into a new wallet with a new set of private keys and related shards.</li> <li>• Private key shards are never combined into a single key and are managed within the banking organizations’ overall</li> </ul>

<i>Key Principle</i>	<i>Application to Crypto-assets</i>
	<p>control framework for safekeeping financial assets. This framework includes ensuring that critical information is encrypted and properly stored and client instructions are communicated and verified through secure channels.<sup>23</sup> Private key shards are stored using separate technology systems, providing an additional layer of control and assurance that the asset cannot be inappropriately access or compromised.</p> <ul style="list-style-type: none"> <li>• Banking organizations would ensure that no one employee has access to all of the key shards to control potential internal malfeasance.</li> </ul>

## **B. Legal risks**

SAB 121’s justification for requiring a safeguarding liability to be recognized on the balance sheet are related, in part, to concerns arising from questions surrounding how such arrangements would be treated in a court proceeding arising from adverse events (e.g., fraud, loss, theft or bankruptcy). Banking organizations have a long history of addressing these risks, which are not new, through well-developed legal, contractual and risk management measures.

### **1. Legal Risk with Respect to Fraud, Loss and Theft**

While many of the risks with respect to fraud, loss and theft are already mitigated by the policies and processes of banking organizations described above, these risks are also contractually allocated between a banking organization and its customer. Importantly, a significant aspect of custody arrangements is risk sharing established by negotiated contractual arrangements between a custodian and its customers.<sup>24</sup> In general, the contracts set out the scope of the services that the custodian will provide to its customer(s), the standard of care that the custodian will exercise in carrying out its duties, and the governing law of the contractual relationship. The terms of these contracts describe allocation of the legal risks of fraud, loss and theft for safeguarded assets as between the banking organization and their customers. The terms of a custody agreement also typically include limitations on liability and disclosures about the risks

<sup>23</sup> Secure messaging to deter inappropriate access to financial assets is a well-established industry practice (e.g., SWIFT messages for the movement of cash and securities).

<sup>24</sup> OCC, *Comptroller’s Handbook: Custody Services* (Jan. 2002) at 8.

a customer faces. In cases where a banking organization uses a sub-custodian, the risks and obligations of each also may be defined by contract and disclosed to the customer.<sup>25</sup>

For activities ancillary to safekeeping activities, such as referral and other finder activities, the customer would enter into contractual agreements directly with the third-party custodian. The third-party custodian would be responsible for safekeeping services (including maintaining cryptographic key information in the case of crypto-assets) and the banking organization would not have any contractual liability for executing trades or safeguarding assets and would include appropriate disclosures and disclaimers in relevant materials made available to customers.

Thus, in all cases, banking organizations would document clearly and disclose to customers their rights and responsibilities under any custody arrangement involving crypto-assets, thereby mitigating the legal risks associated with such activities.

## **2. Legal Risks with Respect to Insolvency**

With respect to legal risks in insolvency, there are multiple legal bases to conclude that safeguarded assets are not the property of the custodian upon such events, specifically: (1) treatment under the UCC"; (2) case law regarding the insolvency of banking organizations that held assets under custody; and (3) regulatory and supervisory guidance applicable to banking organizations that safeguard customer assets. These legal bases work together with contractual provisions to offer relative certainty that custodial assets will not be treated as assets of the custodian.<sup>26</sup> Each of these points are discussed below.

Requiring banking organizations to place an indemnification-like asset on balance sheet invites investor and creditor confusion with respect to the treatment of custodial assets and creates less efficiency in the financial markets.<sup>27</sup> This confusion could carry through to litigation, as the accounting treatment could be cited as undermining the longstanding precedent that provides

---

<sup>25</sup> For example, a U.S. customer may own foreign securities through a U.S. banking organization that relies on a foreign sub-custodian to hold the securities. The U.S. banking organization would disclaim liability if the foreign sub-custodian fails to protect the securities (other than as provided for under applicable law). In other cases, the banking organization may open an account for the benefit of its customers at the sub-custodian, without disclosing the sub-custodian to its customers. However, in both cases, the banking organization is subject to stringent due diligence and monitoring requirements with respect to the foreign sub-custodian and must ensure that the sub-custodian has proper internal controls to protect assets. OCC, *Comptroller's Handbook: Custody Services* (Jan. 2002) at 16.

<sup>26</sup> Indeed, the Banking Agencies have acknowledged that "collateral would generally be considered to be bankruptcy-remote if the custodian is acting in its capacity as a custodian with respect to the collateral". 83 Fed. Reg. 64660, 64684 (Dec. 17, 2018).

<sup>27</sup> For example, the FDIC historically has taken the view that, as receiver of a failed bank, it would honor the customer's custodial claim on Treasury bills only if the bank has not carried the bills as an asset on its own balance sheet. FDIC Advisory Op. No. 88-14 (Feb. 4, 1988).

that custodians have no ownership interest in the custodied assets. In fact, these precedents are often relied upon today in many legal opinions that are issued by law firms in connection with financial transactions to provide comfort to the parties' that the property interests in collateral or margin will be protected in insolvency.

a. Treatment Under the UCC

There is well-established legal precedent in the United States that the determination of property rights in the assets of the entity in resolution is a matter of state law.<sup>28</sup> State law, in turn, includes precedent that supports the conclusion that assets held in custody are not the property of the custodian. For example, most states adopt the uniform version of the UCC, which provides one important basis under which courts have held that custodied assets are property of the customer and not of the custodian.

Specifically, under UCC Article 8-503(a), financial assets held by a securities intermediary (*i.e.*, custodian) to satisfy securities entitlements for entitlement holders (*i.e.*, customers) are not property of the securities intermediary and are not subject to claims of creditors of the securities intermediary. Under UCC Article 8-102(9), a "financial asset" includes any property that is held by a securities intermediary for another person in a "securities account" if the parties have expressly agreed that the property is to be treated as a financial asset under UCC Article 8.

Even though it appears that crypto-assets may be regarded as a "financial asset" for this purpose, there are legislative initiatives underway to clarify the treatment of crypto-assets held under custody.<sup>29</sup> A key premise of the revisions is that, like with other financial assets, crypto-assets falling within the scope of UCC Article 8 and UCC Article 12 would not constitute property of an intermediary.

b. Case Law Regarding the Insolvency of Bank Custodians

In addition to the UCC, other longstanding legal precedents applicable to banking organizations help ensure that, as a matter of law, the property held for customers in safekeeping is not subject to the claims of unsecured creditors in the event of a bank insolvency. Unlike nonbanks, banks

---

<sup>28</sup> See *Butner v. United States*, 440 U.S. 48, 54, 99 S. Ct. 914, 918, 59 L. Ed. 2d 136 (1979); *O'Melveny & Meyers v. FDIC*, 512 U.S. 79, 86-87 (1994).

<sup>29</sup> The amendments were approved by the members of the American Law Institute at the Institute's Annual Meeting and are expected to be approved by the members of the Uniform Law Commission at the Commission's Annual Meeting in July 2022. Thereafter, the amendments may be adopted by each of the states into state law.

are generally not eligible to become Chapter 7 and Chapter 11 debtors under the Bankruptcy Code and, instead, are subject to federal or state insolvency regimes, as applicable.<sup>30</sup>

A well-established principle of federal banking law is that custodial assets are not generally available to creditors of an insolvent bank. By statute and court interpretations, the FDIC, as receiver, generally “takes no greater rights in the property than the insolvent bank itself possessed.”<sup>31</sup> In cases involving a “special deposit”, courts have held that the assets held as special deposits are not assets of the bank and that the customer is not a general creditor of the failed custodian bank.<sup>32</sup> Two related requirements for assets to be treated as special deposits in the existing case law are that the custodian must segregate the assets from its own assets and that commingling of assets does not occur.<sup>33</sup> Although, to our knowledge, no court to date has

---

<sup>30</sup> For brevity, we focus on federal insolvency regimes in this attachment. Additional detail on the legal precedents applicable to banking organizations, such as UCC, contract and insolvency law, can be found in Appendix C (Legal Precedents Applicable to Banking Organizations) of the Banking Agency Letter.

<sup>31</sup> See *Tobias v. Coll. Towne Homes, Inc.*, 110 Misc. 2d 287, 293, 442 N.Y.S.2d 380, 385 (Sup. Ct. 1981) (noting that this would be true unless there is a specific statutory instruction to the contrary). See also 12 U.S.C. § 1821(d)(2)(A)(i); *O’Melveny & Myers v. FDIC*, 512 U.S. at 87; *Peoples-Ticonic Nat. Bank v. Stewart*, 86 F.2d 359, 361 (1st Cir. 1936) (holding that “[a] receiver of a national bank takes title to the assets subject to all existing rights and equities”); *In re Int’l Milling Co.*, 259 N.Y. 77, 83, 181 N.E. 54 (1932) (holding that the New York Superintendent of Banks, when he took over the bank for the purpose of liquidation, acquired no greater interest in the fund than the bank possessed); *In re De Wind*, 144 Misc. 665, 666, 259 N.Y.S. 554 (Sur. 1932) (holding that the trust company never obtained title to the trust funds and title thereto did not pass to the New York Superintendent of Banks when he took over the assets of the trust company); *Williams v. Green*, 23 F.2d 796, 798 (4th Cir. 1928) (holding that the receiver takes the assets of the bank subject to all claims and defenses that might have been interposed as against the insolvent corporation before the liens of the United States and of general creditors attached); *Corn Exch. Bank v. Blye*, 101 N.Y. 303, 303, 4 N.E. 635 (1886) (holding that “[a] receiver of an insolvent national bank acquires no right to property in the custody of the bank”).

<sup>32</sup> See *Merrill Lynch Mortg. Cap., Inc. v. FDIC*, 293 F. Supp. 2d 98, 110 (D.D.C. 2003) (finding under state non-insolvency law that the custodial account was a special deposit entitling the depositor to full recovery and priority over uninsured deposit claims in the receivership proceedings of the failed bank); *In re Mechanics Tr. Co.*, 19 Pa. D. & C. 468, 470 (Com. Pl. 1933) (making a similar finding under applicable state non insolvency law in the context of a bank receivership); *People v. City Bank of Rochester*, 96 N.Y. 32, 34 (1884) (same). Note also that court review of such claims generally must wait until after the FDIC’s administrative claims process (*i.e.*, the court may review *de novo* the FDIC’s administrative claims determinations related to special accounts only after the FDIC’s administrative claims process). See 12 U.S.C. § 1821(j); *Bank of Am. Nat. Assn. v. Colonial Bank*, 604 F.3d 1239, 1246 (11th Cir. 2010).

<sup>33</sup> See, *e.g.*, *Merrill Lynch Mortg. Capital, Inc. v. FDIC*, 293 F. Supp. 2d 98 (D.D.C. 2003) (“While an implicit agreement could theoretically suffice to overcome the general deposit presumption, the existence of a written agreement—explicitly obligating the bank to segregate deposited funds and leaving legal title with the depositor—seems to be, practically, the dispositive issue in deciding whether a deposit is special.”); *Peoples Westchester Sav. Bank v. FDIC*, 961 F.2d at 331 (finding no special deposit in part because “documents generated in opening the [account] do not evidence that [the bank] assumed a duty to segregate those funds from its own general assets” and “that there was no explicit agreement . . . to segregate [deposited] funds”); *Keyes v. Paducah & I.R. Co.*, 61 F.2d 611, 613 (6th Cir. 1932) (finding no special deposit because the court “fail[ed] to find in any . . . instruments . . . any indication that it was the intention . . . of the parties that the avails of the draft were to be segregated and kept as a separate fund . . .”).

taken a position on whether crypto-assets may be special deposits, the OCC and courts have made clear that special deposits “may be money, securities, or other valuables.”<sup>34</sup>

### **3. Regulatory and Supervisory Guidance Require Mitigation of Legal Risks**

The well-established principles discussed above have led to requirements for regulated banking organizations to address the legal risks of safekeeping activities by segregating assets held in safekeeping so they are not treated as assets of the banking organization in insolvency and the customer does not become a general creditor of a failed custodian.

The OCC’s recent interpretive letter permitting national banks to custody crypto-assets with the agency’s approval states:

A custodian’s accounting records and internal controls should ensure that assets of each custody account are kept separate from the assets of the custodian and maintained under joint control to ensure that an asset is not lost, destroyed or misappropriated by internal or external parties. Other considerations include settlement of transactions, physical access controls, and security servicing. Such controls may need to be tailored in the context of digital custody.<sup>35</sup>

This approach is consistent with current regulations requiring segregation of all assets held by a national bank acting as custodian or fiduciary. For example, 12 U.S.C. § 92a(c) and 12 CFR 9.13(b) generally require that national bank fiduciary account assets be kept separate from bank assets. The OCC’s Part 9 regulations and OCC guidance also require maintenance of accounting records and internal controls that ensure that these requirements are met.<sup>36</sup> Many states have incorporated the OCC’s fiduciary standards into their own banking laws.<sup>37</sup>

The Banking Agencies also have significant expectations regarding non-fiduciary custody activity, including, for example: (1) separation and safeguarding of custodial assets; (2) due diligence in selection and ongoing oversight of sub-custodians; (3) disclosure in custodial contracts and agreements of the custodian’s duties and responsibilities; and (4) effective policies, procedures and internal controls for the proper maintenance of internal books and records, the daily reconciliation of assets with the various entities in the chain of custody, the

---

<sup>34</sup> OCC Conditional Approval No. 479 (July 27, 2011). *See, e.g., Montgomery v. Smith*, 226 Ala. 91, 93, 145 So. 822, 824, 1933 Ala. LEXIS 488, \*8; 5B Michie Banks and Banking Deposits Sec. 330.

<sup>35</sup> OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020) at 10.

<sup>36</sup> OCC, *Comptroller’s Handbook: Custody Services* (Jan. 2002) at 15; OCC, *Comptroller’s Handbook: Asset Management Operations and Controls* (Jan. 2011) at 16.

<sup>37</sup> *See, e.g.,* Cal. Fin. Code § 1560 (West).

deployment of robust data privacy and cybersecurity controls, and the maintenance of comprehensive business continuity and resiliency protocols. These regulatory standards effectively require banking organizations to address the legal risks to customers of safekeeping crypto-assets cited by SAB 121 because they focus on protecting client assets from loss due to bankruptcy or insolvency of a custodian and enhance the safety and soundness of the banking organization engaged in the safekeeping activity.<sup>38</sup> These standards also mitigate the risks associated with fraud and inaccurate or improper accounting. By contrast, there are no similar regulations or requirements for nonbanks that provide crypto-asset safekeeping services today.

### C. Regulatory risks

Banking organizations must follow the same due diligence, risk review and risk management processes when engaging in all activities, including when providing custody services. To help ensure compliance with custody regulations and supervisory standards, bank examiners are required to determine whether a banking organization has adequate systems in place to identify, measure, monitor and control risks, including policies, procedures, internal controls and management information systems.<sup>39</sup> Thus, banking organizations must establish, maintain, and enforce policies and procedures that assess technological, legal and regulatory risks prior to engaging in any new activities, including crypto-asset safekeeping activities. In addition to these requirements, banking organizations are subject to stringent prudential regulation, including capital, liquidity, stress testing and other financial resiliency requirements (on top of general principles of safety and soundness). The prudential oversight of banking organizations ensures that all activities and operations, including safekeeping, are conducted in a safe and sound manner through proper assessment and management of risk, including when using new technologies. This oversight includes the robust evaluation and management of IT risk, the implementing of proper internal controls, the adequate assessment of potential legal risk, the operation of comprehensive cybersecurity programs and the identification and mitigation of potential conflicts of interest. Banking organizations must also meet expectations with respect to other operational resiliency obligations, recovery and resolution planning mandates,<sup>40</sup> and

---

<sup>38</sup> 84 Fed. Reg. 17967, 17970 (Apr. 29, 2019).

<sup>39</sup> OCC, *Comptroller's Handbook: Custody Services* (Jan. 2002). Notably, the handbook highlights that operational risk is inherently high in custody services because of the high volume of transactions processed daily. Accordingly, banking organizations already understand that effective policies and procedures, a strong control environment and efficient use of technology are essential risk management tools that must and should be applied to crypto-asset custody activities.

<sup>40</sup> Banking organizations are subject to exams that evaluate how well management addresses risk related to the availability of critical financial products and services, including cyber events, and requires adoption of processes for management to oversee and implement resilience, continuity and response capabilities to safeguard employees, customers and products and services. See FFIEC, *FFIEC Information Technology Examination Handbook: Business Continuity Management* (Nov. 2019).



anti-money laundering and financial crimes regulation.<sup>41</sup> Adherence to these standards is monitored by the oversight and review of dedicated teams of on and off-site examiners from the Banking Agencies. This risk management framework distinguishes banking organizations from nonbanks, protects clients and promotes safety and soundness regardless of the activity in which a banking organization is engaged. As a result, banking organizations, including those that provide safekeeping services, are a key source of stability in the financial ecosystem and ensure high levels of investor protection.

---

<sup>41</sup> See, e.g., FFIEC, BSA/AML Examination Manual, available at <https://bsaaml.ffiec.gov/manual>.

## Attachment B

### Summarized Fact Patterns Expected to be Provided to OCA Staff on a Future Date

The following summarizes certain specific fact patterns we expect to raise in due course to the Staff to help clarify the scope of SAB 121.

#### Definition of Crypto-Assets

1. The definition of “crypto-assets” is very broad and, as a result, it can be challenging to determine what products and activities are in scope of SAB 121 and, therefore, could be interpreted to apply to crypto-assets with risks that are not significantly different than traditional (*i.e.*, non-crypto) forms of assets. Crypto-assets exist in various forms with different characteristics. For example, there is generally a difference between blockchain technology defining the asset itself (*e.g.*, a cryptocurrency such as bitcoin) versus simply being a mechanism to record a right to something of distinct value, such as ownership of securities. This distinction is important because it can impact the legal rights and obligations of the parties to a given transaction as well as inform the evaluation of the risks involved in holding such crypto-assets, either directly or when acting in a safeguarding capacity for clients.
2. Of particular focus are certain transactions that utilize distributed ledger technology to effect settlement and act as a digital record or register of ownership in an asset, such as financial securities. For example, within the context of regulated financial institutions, “tokenized assets” reference traditional assets and operate within the existing infrastructure and legal and regulatory frameworks with appropriate checks and controls, and typically use **permissioned blockchains**. Tokenized assets – including digitally native versions of traditional assets – are particularly secure with respect to technological risks because permissioned blockchain networks incorporate strict governance and control mechanisms, as discussed below. This activity is growing significantly as, among other things, it can lead to more efficient settlement processes with improved speed and data security as well as reduced costs, particularly around reconciliation.<sup>42</sup> From a legal perspective, our understanding is that the tokenization process generally does not create or represent a new type of financial product; rather, the terms and conditions and legal rights and obligations of the underlying financial security prevail, with blockchain used merely as a register to maintain the record of

---

<sup>42</sup> See <https://www.marketsmedia.com/state-street-digital-takes-first-step-on-the-moon>; <https://www.dtcc.com/news/2021/november/09/dtcc-to-launch-platform-to-digitalize-and-modernize-private-markets>; and <https://www.goldmansachs.com/insights/pages/from-briefings-10-june-2021.html>.

ownership. Further, safeguarding such financial securities subject to tokenization is not understood to have significant incremental risk from a price / volatility perspective. As a result, practice has generally looked-through to the underlying securities (or assets more generally) to inform the appropriate accounting treatment, and accounting for the safeguarding of such securities has not been viewed differently than the safeguarding of the same securities in the traditional (*i.e.*, non-crypto) sense.

SAB 121, however, does not make a distinction between the various forms of crypto-assets, particularly those that do not present the risks identified in the guidance; therefore, we expect to raise several fact patterns in this specific context (*e.g.*, consistent with those footnoted above) for analysis.

3. Another example of using blockchain technology to effect transactions involves the **tokenization of cash deposits**.<sup>43</sup> For example, a banking entity may create such tokens using permissioned blockchain technology (*i.e.*, one that can only be accessed by users with permissions, where users can only perform specific actions granted to them by the administrator) that represent customers' account balances with respect to deposits legally owned by the customer.

When using a permissioned blockchain, a banking entity generally is able to maintain control over transactions in the same way as is possible with transactions recorded on any other electronic ledger system of the banking entity today. Specifically, the banking entity controls the operational procedures and the code, and controls all access to and user permissions on the platform. Depending on the design and intended use of the blockchain system, the banking entity may also control the extent to which participants on the platform may view the blockchain ledger and the underlying asset that the digital asset represents. Ultimately, the blockchain technology acts as payment rails and deposit account ledgers, so that clients can instantaneously transfer cash held on deposit.

In these cases, the banking entity has already recognized a liability representing its obligation to return the cash received and, therefore, it would seem counterintuitive to recognize a second liability for this activity, particularly where the banking entity has the ability to “**cancel and correct**” erroneous activity. In other words, given this ability, it would not seem the entity can lose the deposit twice and, therefore, we assume this activity is outside the scope of SAB 121.

---

<sup>43</sup> See <https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments> and <https://newsroom.wf.com/English/news-releases/news-release-details/2019/Wells-Fargo-to-Pilot-Internal-Settlement-Service-Using-Distributed-Ledger-Technology/default.aspx>.

SAB 121 does not provide clarity on this type of activity, including what characteristics may adequately address the risks identified by the Staff such that the activity is not in scope of the guidance (*e.g.*, **permissioned versus non-permissioned**) and, therefore, we expect to raise this as a fact pattern for analysis.

4. Another example of using blockchain technology to effect transactions involves the **tokenization of repurchase (“repo”)**<sup>44</sup> and **securities borrow-pledge transactions**. Focusing on the former and similar to the concept discussed above, blockchain technology is used to define tokens for (1) cash held in a segregated account and (b) an underlying security, such as a US Treasury, held in another segregated account. An exchange of such tokens is representative of an exchange of cash and collateral and, therefore, blockchain acts as a new set of rails on which cash and collateral are moving. For example, in the case of cash, rather than needing to instruct cash movements via the SWIFT network and local payment systems, parties can simply exchange tokens representative of the underlying cash. It is important to note that neither cash tokens nor collateral tokens are a form of cryptocurrency, the primary difference being that the tokens are a representation of the assets only and where the use of blockchain technology does not change the legal rights, characteristics or form of the underlying assets itself<sup>7</sup>. Further, the transactions remain subject to standard Master Repurchase Agreement terms and conditions.

Given blockchain technology is used for record-keeping purposes of underlying traditional assets and transactions therein (*e.g.*, sales and exchanges), we believe that the accounting treatment applied to such transactions should be the same as the existing GAAP applied and there should not be any incremental accounting imposed on any party responsible for safeguarding the tokens. SAB 121, however, does not distinguish these types of assets from other crypto-assets and, therefore, we expect to raise both of these activities as fact patterns for analysis.

#### Nature of Roles and Responsibilities

5. We believe clarity would also be helpful regarding the types of safeguarding activities that are in scope of SAB 121. For example, in addition to the various forms of sub-custody and referred custody (*i.e.*, where an entity simply introduces a client to a third-party who will provide safeguarding services directly to the client) which we understand have already been highlighted to the Staff, we believe clarity would also be helpful

---

<sup>44</sup> <https://www.bloomberg.com/news/articles/2021-06-22/goldman-sachs-begins-trading-on-jpmorgan-repo-blockchain-network#xj4y7vzkg>.

regarding safeguarding of tokenized assets (as discussed above) as well as where entities act in **fiduciary capacities** to vehicles or trusts that hold crypto-assets; for example:

- a. An investment manager arrangement where the fiduciary (i.e., investment manager) has access to private keys and may transact on behalf of a trust, etc.;
- b. The Trust and trustee does not have access to the private keys but is legally empowered to instruct a crypto-asset custodian on behalf of a trust; or
- c. The Trust, on instructions of a client, opens a third-party account that may transact in crypto-assets, noting in this case there would be no direct access to the crypto-assets; rather, the client would have access.

#### Entity-Specific Considerations<sup>45</sup>

6. In all cases, we believe the technological, legal and regulatory risks highlighted in SAB 121 may be sufficiently mitigated depending on the nature of the entity providing safeguarding services. For example, on December 23, 2020, the SEC issued a statement<sup>46</sup> describing certain conditions under which a **special purpose broker-dealer** could comply with the requirements of Rule 15c3-3 under the Securities Exchange Act of 1934 with respect to digital asset securities. We believe it would be helpful to understand if an entity that meets these or similar conditions would be outside the scope of SAB 121.

---

<sup>45</sup> This is in addition to confirming more broadly that the risks outlined in SAB 121 are sufficiently mitigated for banking organizations because of the stringent regulatory and supervisory frameworks within which they operate and, therefore, the guidance should not be applied, as discussed in Attachment A.

<sup>46</sup> See generally <https://www.sec.gov/news/press-release/2020-340>.

## Attachment C

### Questions Regarding Recognition, Measurement and Disclosure of the Safeguarding Liability

We understand that certain of the following questions regarding the recognition, measurement and disclosure of the safeguarding liability requirements of SAB 121 may have already been raised to the Staff (*e.g.*, through discussions with the DAWG); however, we believe a lack of clarity remains and our member firms would benefit from direct feedback from the Staff.

1. Please clarify the model / framework by which a safeguarding liability is recognized. For example, one framework that may apply in this case is the guidance on the recognition and measurement of loss contingencies (*i.e.*, ASC 450-20), which contemplates recognition where it is probable a loss has been incurred and the amount of loss can be reasonably estimated – is this the appropriate model to apply to the safeguarding liability? If so, we do not believe the particular technological, legal and regulatory risks of the crypto-assets suggest the potential loss or “sacrifice” is probable, nor would we estimate that the estimated loss corresponds to the entire balance subject to safeguarding. Alternatively, if the loss contingency guidance is not the basis for recognition and measurement of the safeguarding liability, please specify the appropriate accounting framework as it will help address some of the additional questions we outline below.
  
2. Our interpretation of SAB 121 is that the initial and subsequent measurement of the safeguarding liability should be at the fair value of the crypto-assets the entity is deemed responsible for holding, and not the fair value of the safeguarding liability itself. With this in mind, when measuring an entity’s own financial obligations at fair value, one generally considers the impact of time value, entity-specific credit risk and other valuation adjustments within the context of determining the value at which the obligation could be exited to relevant market participants. Our understanding is that such adjustments and concepts are not applicable in this case, but we believe clarification is necessary, including whether the safeguarding liability is considered a financial liability. If our interpretation is correct that the safeguarding liability should only be measured at the fair value of the crypto-assets the entity is responsible for holding, guidance is needed as to how this fair value should be derived. For example, if the crypto-asset is a cryptocurrency that is traded on an exchange, cryptocurrencies are traded on multiple exchanges and around the clock. In this instance, how should the principal market be determined? Further, there could be diversity in practice on which quote should be used as the fair value measurement – the highest price, the lowest price

or any other price. To achieve comparability, guidance should be provided on this and other aspects (*i.e.*, measurement of the recognized asset), including that fair value should be determined as of a balance sheet date.

3. We understand that the measurement of the safeguarding liability is impacted by the extent to which the underlying crypto-assets that are being safeguarded continue to be safeguarded by the entity. With this in mind, assume theft has resulted in the safeguarding entity losing all of the crypto-assets previously safeguarded. In this case, if the safeguarding entity is not contractually required to make its clients whole and elects not to do so, we believe the liability should be released at such time. Thereafter, we believe the safeguarding entity would apply the loss contingency model (*i.e.*, ASC 450-20), to capture the potential loss resulting from any future litigation. If this interpretation is not correct, additional guidance is needed to articulate how the safeguarding liability is released.
4. SAB 121 indicates that (**emphasis added**) “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... including an **increased risk of financial loss**” as part of the basis as to why an entity should present a liability on its balance sheet to reflect its obligation to safeguard crypto-assets.

Given the language referenced above and the fact that the asset recognized is not the crypto-asset itself (*i.e.*, as might otherwise be recognized if the entity that is safeguarding the crypto-assets was deemed the accounting owner based on an analysis of control, economics, etc.), we believe that the safeguarding liability is a representation of the financial loss and should be evaluated accordingly when considering its classification. In other words, this may suggest the safeguarding liability is long-term in nature (*i.e.*, because while theft could occur at any time, the point at which the loss is realized and becomes due may play out over an extended period of time, including if there is an expectation that it will be subject to litigation) as opposed to short-term in nature (*i.e.*, because the client can withdraw the crypto-assets on demand and, therefore, the entity’s obligation to perform is potentially real-time). However, if our interpretation is not correct, additional guidance is necessary to articulate what is relevant to this analysis.