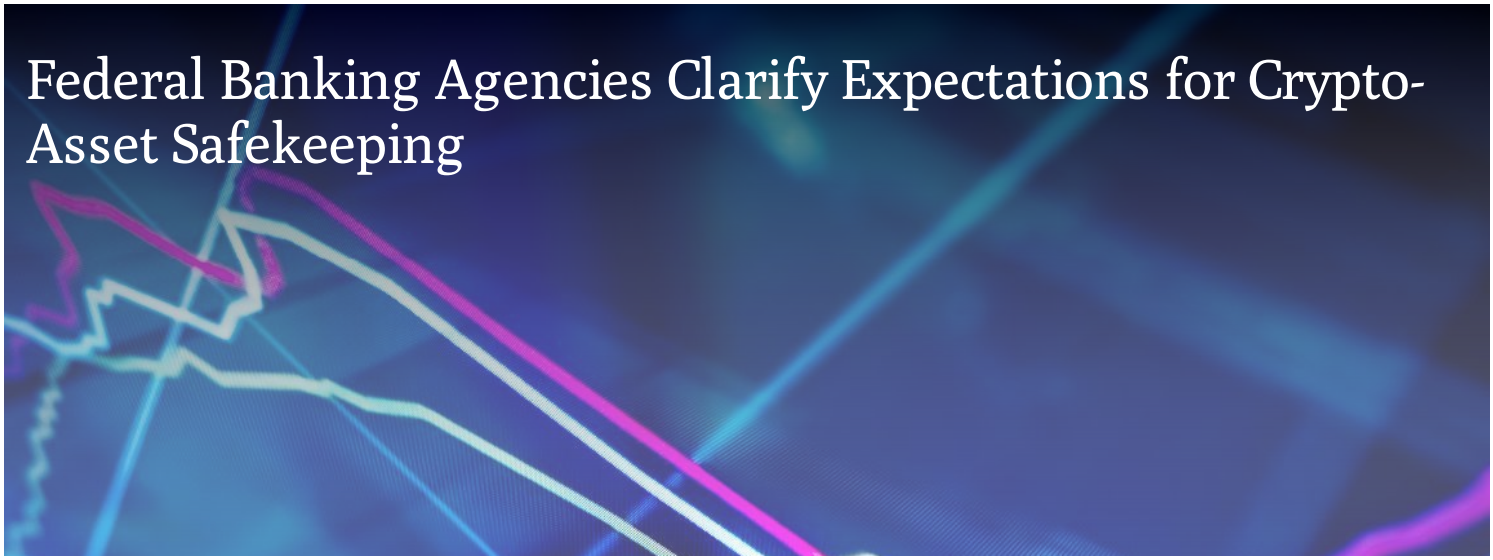
WINSTON & STRAWN LLP

CLIENT ALERT

Federal Banking Agencies Clarify Expectations for Crypto-Asset Safekeeping



JULY 18, 2025

The Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (Board), and the Federal Deposit Insurance Corporation (FDIC) (together, the "**Agencies**") have issued a joint statement clarifying the regulatory expectations applicable to the safekeeping of crypto-assets by banking organizations. The interagency statement (the "**Safekeeping Guidance**") offers a structured articulation of how legacy supervisory principles are expected to operate in the emerging context of crypto-asset safekeeping by banking organizations.

NEW SERVICE RISK ASSESSMENT AS A FOUNDATIONAL OBLIGATION

Although the OCC's "New, Modified, or Expanded Banking Products and Services: Risk Management Principles" guidance applies on its face only to OCC-supervised banking organizations, the Safekeeping Guidance directs Board- and FDIC-supervised banking organizations to follow it as well.[1]

This means that federal banking organizations are expected to conduct a comprehensive and forward-looking risk assessment prior to offering crypto-asset safekeeping services. This risk assessment must evaluate whether crypto-asset safekeeping services align with the organization's strategic direction and risk profile, assess the organization's ability to understand and control a complex and still-maturing asset class, and determine whether its operational capacity and governance model can support the service in a safe and sound manner.

Critically, the Safekeeping Guidance underscores the importance of contingency planning for crypto-asset safekeeping services, citing contingency planning for lost cryptographic keys as an illustrative example. This reflects a supervisory expectation that banking organizations have contingency plans grounded in the specific risks identified during the risk assessment of the crypto-asset safekeeping service. Banking organizations should therefore not assume that legacy business continuity and disaster recovery plans or cybersecurity incident response plans can be repurposed wholesale. Examiners will expect both a clear understanding of crypto-asset risks and a demonstrable commitment to adapting governance and controls accordingly.

CRYPTO-ASSET RISK ASSESSMENTS

In addition to evaluating the crypto-asset safekeeping service as a whole, the Safekeeping Guidance sets a clear expectation that banking organizations will conduct individualized risk assessments for each crypto-asset they

intend to support. This expectation echoes the virtual currency listing guidance that has been in place for virtual currency entities supervised by the New York Department of Financial Services (since 2020).[2]

For each crypto-asset a banking organization intends to support, the Safekeeping Guidance establishes an expectation that the banking organization conduct an analysis of the crypto-asset's technical, operational, legal, market, and strategic characteristics. Banking organizations are also expected to remain current on material developments affecting the crypto-assets they support, including changes to the underlying ledger technology or governance structure.

From a practical standpoint, this expectation will require many banking organizations to create internal digital asset review committees or working groups, with the appropriate technical, legal, and compliance expertise. Reliance on third-party sub-custodians or analytics tools will not absolve institutions of the need to own and document their risk conclusions. As a result, both vendor diligence and internal governance functions will need to mature in parallel.

CRYPTO-ASSET CUSTODY AND SAFEKEEPING AGREEMENTS

The Safekeeping Guidance identifies the customer agreement as a critical component of the risk management framework. While this may be routine in the context of traditional custody services, the specific provisions identified in the Safekeeping Guidance highlight that crypto-asset safekeeping introduces a number of new legal and operational risk scenarios to be addressed.

A well-drafted agreement should address issues including on-chain governance and voting rights, forks and airdrops, probabilistic settlement on permissionless blockchains, methods of digital asset storage (cold, hot, or hybrid wallets), the use and liability structure of sub-custodians, and the deployment and oversight of smart contracts.

This expectation has practical implications for legal and compliance teams. Traditional templates may need to be reengineered to accommodate new provisions. Legal teams will need to coordinate closely with product, operations, and risk functions to ensure that the terms of the agreement contain provisions that align with the technical aspects of the organization's safekeeping solution and its accounting structures. For example, the Safekeeping Guidance leaves the decision to banking organizations whether to use omnibus or segregated accounts, but that decision has implications on technical design and the language for account titling and segregation in the agreement.

CLARITY IN DISCLOSURES: AVOIDING MISINFORMATION IN A FRAGMENTED ECOSYSTEM

The Safekeeping Guidance also underscores the risk of customer confusion regarding the banking organization's role in crypto-asset safekeeping arrangements, particularly when third-party providers or sub-custodians are involved. The Agencies expect that banking organizations will provide customers with clear, timely, and accurate information about the nature of the safekeeping relationship, including whether the bank participates in governance decisions, how assets are stored, and which parties are responsible for key control and transactional authority.

This expectation demands more than mere legal disclaimers. Banking organizations should assess their marketing materials, digital interfaces, onboarding documentation, and customer service protocols to ensure consistency and clarity.

"STANDARD" RISK MANAGEMENT PRINCIPLES APPLY, BUT TECHNICAL EXPERTISE IS STILL NECESSARY

Perhaps the most critical theme running throughout the Safekeeping Guidance is that while established custodial risk management principles still apply, their effective implementation in the context of crypto-assets implicitly requires expertise in crypto-assets.

Importantly, this expertise cannot simply be siloed within the information technology team. Institutions must ensure that crypto-asset literacy extends to the appropriate business units (First Line of Defense), the independent risk management function (Second Line of Defense), and the internal audit function (Third Line of Defense). The Agencies place particular emphasis on the audit and control functions, which must be capable of addressing the unique technical aspects of crypto-asset safekeeping, including cryptographic key generation and destruction,

transaction settlement finality, wallet architecture, and smart contract behavior. The Agencies note that where internal expertise is lacking, institutions are expected to engage independent third-party resources with sufficient qualifications and independence to assess crypto-asset safekeeping operations. For many institutions, this will require both immediate resource investments and a longer-term strategy for talent development.

NOTABLE OMISSIONS: WHAT THE SAFEKEEPING GUIDANCE LEAVES UNSAID

Despite its breadth, the Safekeeping Guidance is notably silent on several areas. Banking organizations should not misconstrue these omitted topics as de facto safe harbors.

First, the Safekeeping Guidance does not address the FDIC's heightened scrutiny of deposit insurance representations in the digital asset context. Given the FDIC's moves to amend and expand its deposit insurance–related advertising regulations over the past several years, institutions must continue to ensure that any digital asset–related disclosure or interface is in an allowed location so as not to imply that crypto-assets are insured or backed by the U.S. government. The updated regulations have required modifications (and sometimes redesigns) of advertisements, webpages, and user interfaces for traditional banking and brokerage services, and banking organizations intending to offer crypto-asset safekeeping should plan for similar challenges.

Second, the Safekeeping Guidance has no discussion of account titling, despite its importance in determining customer ownership rights during insolvency scenarios. The omission is particularly notable in context, given that proper titling of custody accounts has been a focus over the last three years following multiple high-profile digital asset bankruptcies in 2022. Even if not discussed in the Safekeeping Guidance, proper account titling and account documentation remain critical, both when safekeeping is conducted directly and when sub-custodians are involved.

Third, the Safekeeping Guidance makes only cursory mention of cybersecurity, stating that it should be a "key focus." Banking organizations should not assume that this one-sentence reference reflects the level of organizational investment in cybersecurity and information technology risk functions that will likely be required. To the contrary, we expect these areas to be the ones where banking organizations are in most need of new investment to comply with the supervisory expectations set in the Safekeeping Guidance.

FINAL THOUGHTS

The Safekeeping Guidance marks a significant step in the Agencies' supervisory treatment of crypto-asset activities as the first "real" supervisory guidance to date. While the Safekeeping Guidance confirms that crypto-asset safekeeping is permissible under existing laws and is subject to traditional risk management principles, it also makes clear that offering crypto-asset safekeeping services in a compliant manner will require much more than just adapting legacy systems and risk management frameworks. The Safekeeping Guidance makes clear that the Agencies expect banking organizations to engage deeply with the unique technical, legal, and operational risks of crypto-assets and to demonstrate the capacity to manage those risks at every level of the enterprise.

* * * * *

For assistance in evaluating your banking organization's readiness to offer crypto-asset safekeeping or aligning existing operations with supervisory expectations, please contact your Winston & Strawn LLP representative or a member of our Digital Assets Group and Fintech, Banking & Payments Group.

---

[1] *See* OCC Bulletin 2017-43, "New, Modified, or Expanded Banking Products and Services: Risk Management Principles" (Oct. 20, 2017).

[2] *See* "Guidance Regarding Listing of Virtual Currencies" (Nov. 15, 2023); "Guidance Regarding Adoption or Listing of Virtual Currencies" (June 24, 2020) (superseded by Nov. 2023 guidance).

6 Min Read

Authors

Carl Fornaris

Andrew Maxwell Hinkes

Kimberly A. Prior

Daniel T. Stabile

Logan Payne

Related Capabilities

Financial Innovation & Regulation

Financial Services Litigation

Cryptocurrencies, Digital Assets & Blockchain Technology

Financial Services

Related Professionals

Carl Fornaris

Andrew Maxwell Hinkes

Kimberly A. Prior

Daniel T. Stabile

Logan Payne