CADWALADER

CABINET NEWS

Research and commentary on regulatory and other financial services topics

Federal Banking Regulators on Crypto-Asset Safekeeping

July 24, 2025

By Mercedes Kelley Tunstall
Partner | Financial Regulation

Just days prior to the passage of the GENIUS Act on stablecoins by Congress, on July 14th, the Federal Reserve, Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation (collectively, the "Agencies") issued **a joint statement called "Crypto-Asset Safekeeping by Banking Organizations"**. Safekeeping refers to any service provided by banks that involves "holding an asset on a customer's behalf" and safekeeping **of crypto-assets** means controlling the keys associated with the crypto-assets. The Agencies distinguish safekeeping from situations where the bank is a full-fledged custodian of assets (i.e., safekeeping services alone may not rise to the level of causing banks to have a fiduciary duty to the customer). This means that the statement applies whether or not the bank has a fiduciary duty to the customer.

First, the Agencies identify general risk management considerations whenever safekeeping of crypto-assets occurs. Specifically, banks should conduct a risk assessment of engaging in safekeeping crypto-assets that addresses all of the following: 1) core financial risks of safekeeping; 2) the bank's ability to understand the asset class; 3) the bank's ability to ensure a strong control environment; and 4) contingency plans to address unanticipated challenges in effectively safekeeping.

Of crucial importance is that the bank understands the "technology underlying" crypto-assets. Each individual crypto-asset has different smart contracts associated with it, different redemption policies, different reserves (in the case of stablecoins) and a single crypto-asset can be used in multiple ways – some activities could be classified as engaging in commodity transactions and other activities could be viewed as engaging in securities transactions, for example. This means that banks really should conduct a risk assessment of not just engaging in safekeeping activities, but also of each individual kind of crypto-asset it proposes to safekeep.

Additionally, as the Agencies point out, "[o]ne of the primary risks of crypto-asset safekeeping is the possible compromise or loss of cryptographic keys or other sensitive information that could result in the lose of crypto-assets or the unauthorized transfer of the crypto-assets out of the" bank's control. This means that the bank must be ready to face the risks of being held liable for its customers' losses. That liability turns on whether the bank has "control" of the crypto-asset, which the Agencies define as meaning that "no other party – including the customer – has access to information sufficient to unilaterally transfer the crypto-asset". Note that under Article 12 of the UCC, as contained in the 2022 UCC Amendments, it is possible for control to be achieved even in the case of a shared wallet. But, for now, the Agencies are clearly stating that "control" of a crypto-asset happens when only one party has the ability to cause transfer of the crypto-asset.

Finally, the Agencies underscore the need for careful compliance with anti-money laundering laws and compliance with Office of Foreign Asset Control requirements, to which "[t]he design features of distributed ledger technology may present challenges for achieving or maintaining compliance."