Articles + Publications | April 25, 2022

Not Your Keys, Not Your Coin: SEC Tells Crypto-Custody Providers to Report Platform Users' Crypto Holdings as Balance Sheet Liabilities

WRITTEN BY

Keith J. Barnett | Ethan G. Ostroff | Kalama M. Lui-Kwan | Ghillaine A. Reid | Carlin A. McCrory | Elizabeth P. Waldbeser | Jay A. Dubow | Addison J. Morgan

On March 31, the Securities and Exchange Commission (SEC) issued Staff Accounting Bulletin No. 121 (Bulletin), noting that a company safeguarding or exerting custody over cryptocurrency on behalf of its platform users must clearly report the users' assets as liabilities on the company's financial statement, along with the risks consumers face by entrusting the company with their private, cryptographic keys.

Public-Key Cryptography. Public-key cryptography is a type of encryption scheme that uses two nonidentical, corresponding keys to encrypt and decrypt data. One of these keys is *public* — like an email address — and can be discovered by any user of a public blockchain. For example, in a peer-to-peer transaction, parties exchange public wallet addresses (*i.e.*, public keys) to facilitate transfer and receipt of crypto-assets. When Party A sends a crypto asset to Party B's public wallet address, Party A is sending Party B encrypted data that lives on the blockchain. To decrypt this data, Party B must have access to the *private key* that corresponds to the public key he provided to Party A. Stated differently, in public-key cryptography, only the private key owner can decrypt encrypted data sent to his or her public key, which affords this person complete control over the underlying crypto-assets.

Practical Considerations. As the Bulletin makes clear, users of entities who hold their crypto-assets in digital wallets provided on the entities' platforms are not the true owners of those crypto-assets as the entities maintain the private, cryptographic keys necessary for platform users to access their crypto-assets. To mitigate risk of exposure to loss of platform users' private, cryptographic keys (which would result in total loss of the underlying crypto-assets), the SEC suggests these entities will be required to engage in certain practices:

- Report the obligation associated with these custody arrangements as liabilities on their balance sheets (safeguarding liability);
- Measure safeguarding liabilities and crypto assets at fair market value at the time of acquisition; and
- Make disclosures concerning the risks associated with entrusting one's cryptographic key information to a third party, such as theft or loss.

The Bulletin requires entities that file with the SEC to comply with this updated guidance by June 15, 2022.

Our Take. Although the Bulletin does not provide a comprehensive regulatory framework, it suggests the SEC perceives *public-key cryptography* as both a unique and potentially hazardous phenomenon.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Payments + Financial Technology
- Securities Investigations + Enforcement
- White Collar Litigation + Investigations