CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

FBI Warns About Cybersecurity Problems on DeFi Platforms

By **Mercedes Kelley Tunstall**
Partner | Financial Regulation

Decentralized finance platforms (DeFi) are designed to operate in a decentralized manner primarily through the utilization of smart contracts. Smart contracts are simply a name given to small "if/then" statements written in computer code that are self-executing. Smart contracts are used throughout the cryptocurrency and blockchain space, are an integral component in non-fungible tokens (NFTs), and can allow for things to happen automatically, without human intervention. For example, a smart contract could be coded such that payment for an item could be released upon receipt of a shipment, so **if** the shipment is received, **then** payment is released.

In the case of DeFi platforms, the coded smart contracts allow for trading of cryptocurrency, stocks, and ETFs; funds to be transferred between parties; and even loans to be made that are secured by crypto or other investments. These smart contracts interact with the blockchain, but in most cases are not written to the blockchain, which means that the smart contracts do not enjoy the encryption protection of the blockchain, and are simply computer code that can be manipulated and hacked just like any other computer code, if not properly secured by the DeFi platform. The FBI's August 29, 2022 Public Service Announcement warns the public (*i.e.*, investors) about these smart contract vulnerabilities on DeFi platforms. The PSA reports that in just three months of 2022, "cyber criminals stole $1.3 billion in cryptocurrencies, almost 97 percent of which was stolen from DeFi platforms."

The FBI recommends that investors should seek advice from a licensed financial adviser, but to the extent DeFi platforms will be used, investors should research the DeFi platforms they are using and ensure that the platform has conducted thorough security audits that include a "code audit" and should be alert, in particular, to "DeFi investment pools with extremely limited timeframes." Companies that provide DeFi platforms are urged to step up their cybersecurity

compliance, to conduct a code audit and to develop a robust incident response plan.
