NBA Nebraska Bankers Association

www.nebankers.org

Update COMPLIANCE

November 18, 2022 Vol. XXXIV, No. 27

FRB CRYPTOCURRENCY GUIDANCE – DUE DILIGENCE

I. INTRODUCTION

The Federal Reserve Bank (FRB) has issued a Supervisory Letter indicating that Fed-supervised banks seeking to engage in activities related to cryptocurrency and other digital assets must first assess whether such activities are legally permissible and determine whether any regulatory filings are required. The letter also states that banks should notify the Fed prior to engaging in crypto-asset-related activities. The Supervisory Letter is similar to guidance previously issued by the Office of the Comptroller Currency (OCC) and Federal Deposit of Insurance (FDIC); in all cases, the agencies require banks to notify regulators before engaging in any kind of digital asset activity, including custody activities.

The term "crypto-asset-related activity" includes, at a minimum, crypto-asset safekeeping and traditional custody services, ancillary custody services, facilitation of customer purchases and sales of crypto-assets, loans collateralized by crypto-assets, and issuance and distribution of stablecoins.

The new requirement is set forth in Supervision and Regulation (SR) Letter 22-6, which directs institutions to have "adequate systems, risk management, and controls to conduct crypto-asset-related activities in a safe and sound manner and consistent with applicable laws, including applicable consumer protection statutes and regulations" prior to engaging in crypto activities.

SR 22-6 notes the following risks associated with crypto-asset-related activities related to safety and soundness, consumer protection, and financial stability:

- Technology and operations: The technology underlying crypto-assets is nascent and evolving, and poses novel risks such as those associated with cyber security and governance of the underlying network and any related arrangements. These risks are particularly heightened when the underlying technology involves open, permissionless networks.
- Anti-money laundering and countering of financing of terrorism: Crypto-assets can be used to facilitate money laundering and illicit financing. Some crypto-assets have limited transparency, making it difficult to identify and track ownership.
- Consumer protection and legal compliance: Crypto-assets pose significant consumer risks such as those related to price volatility, misinformation, fraud, and theft or loss of assets. In addition, banking organizations engaging in crypto-asset-related activities face

potential legal and consumer compliance risks stemming from a range of issues, including, for example, uncertainty regarding the legal status of many crypto-assets; potential legal exposure arising from consumer losses, operational failures, and relationships with crypto-asset service providers; and limited legal precedent regarding how crypto-assets would be treated in varying contexts, including, for example, in the event of loss or bankruptcy.

- Financial stability: Certain types of crypto-assets, such as stablecoins, if adopted at large scale, could also pose risks to financial stability including potentially through destabilizing runs and disruptions in the payment systems.

The letter provides that a Federal Reserve–supervised banking organization, engaging or seeking to engage in crypto-asset-related activities should notify its lead supervisory point of contact at the Federal Reserve. Prior to engaging in any crypto-asset-related activity, a supervised banking organization must ensure such activity is legally permissible and determine whether any filings are required under applicable or state laws. Prior to engaging in these activities, a supervised banking organization should have in place adequate systems, risk management, and controls to conduct such activities in a safe and sound manner and consistent with all applicable laws, including applicable consumer protection statutes and regulations.

II. LEGAL PERMISSIBILITY

Prior to engaging in new activities of any kind, a supervised banking organization must ensure that such activities are legally permissible. A supervised banking organization seeking to engage in (or currently engaged in) crypto-asset-related activities must analyze the permissibility of such activities under relevant state and federal laws and determine whether any filings are required under federal banking laws, including the Bank Holding Company Act, Home Owners' Loan Act, Federal Reserve Act, Federal Deposit Insurance Act, or the regulations promulgated pursuant thereto, as applicable. If any supervised banking organization has questions regarding the permissibility of any crypto-asset-related activities or about the applicability of any filing requirements, it should consult its lead supervisory point of contact at the Federal Reserve.

III. NOTIFICATION OF PROPOSED ACTIVITIES

A supervised banking organization should notify its lead supervisory point of contact at the Federal Reserve prior to engaging in any crypto-asset-related activity. Any supervised banking organization that is already engaged in crypto-asset-related activities should notify its lead supervisory point of contact at the Federal Reserve promptly regarding the engagement in such activities, if it has not already done so. Federal Reserve supervisory staff will provide relevant supervisory feedback, as appropriate, in a timely manner.

In all cases, a supervised banking organization should, prior to engaging in these activities, have in place adequate systems, risk management, and controls to conduct crypto-asset-related activities in a safe and sound manner and consistent with applicable laws, including applicable consumer protection statutes and regulations. This includes having adequate systems in place to identify, measure, monitor, and control the risks associated with such activities on an ongoing basis. These systems should cover operational risk (for example, the risks of new, evolving technologies; the risk of hacking, fraud, and theft; and the risk of third-party relationships), financial risk, legal risk, compliance risk (including, but not limited to, compliance with the Bank Secrecy Act, anti-money laundering requirements, and sanctions requirements), and any

other risk necessary to ensure the activities are conducted in a manner that is consistent with safe and sound banking and in compliance with applicable laws, including applicable consumer protection statutes and regulations. State member banks are also encouraged to notify their state regulator prior to engaging in any crypto-asset-related activity.