Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
Phone (312) 382-7500
Fax (312) 382-6901

April 19, 2023

Board of Directors

b4,b8

Subject: Notification of Engagement in Crypto-Related Activities

Dear Members of the Board:

The FDIC acknowledges the notification provided by b4,b8 b4,b8 (the Bank), regarding the Bank's intent to offer a third-party authorization verification service for customer transactions in crypto-assets. The notification was provided pursuant to Financial Institution Letter (FIL), FIL-16-2022 Notification of Engaging in Crypto-Related Activities. FIL-16-2022 requested that all FDIC supervised institutions that intend to engage in, or that are currently engaged in, any activities involving or related to crypto-assets (also referred to as "digital assets") promptly notify the appropriate FDIC Regional Director.

While the notification provides a summary of the proposed activities, the FDIC will need additional documentation to understand what the bank is proposing and to evaluate the safety and soundness, consumer protection, and financial stability considerations of the proposed activities. Enclosed is a request for additional information needed to fully review the proposed activities and provide appropriate supervisory feedback to the Bank. Please respond to the request no later than May 31, 2023.

This letter is confidential and may not be disclosed or made public in any manner under Part 309 of the FDIC Rules and Regulations (12 CFR part 309). If you have any questions, please contact Case Manager b8 at b6,b8 or Review Examiner b8 b8 at b6,b8. Written correspondence should be addressed to my attention at the Chicago Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: CHIMailRoom@FDIC.gov.

Sincerely,
Gregory P. Bottone
Regional Director

cc: b8

ATTACHMENT

Please provide final or draft copies of the following information with respect to *each proposed crypto-asset activity.*

General:

1. The notification letter to the FDIC addressed multiple activities. Provide a detailed and clear description of each activity that the bank proposes to engage in. For example, the letter addressed transaction verifications, node functions, multi-signature processes, and indicated that the bank has been informed it will not be custodian. Please clarify which of these functions the bank will perform and provide supporting information as follows:
    - Description of how the bank will verify transactions.
    - Description of whether the bank will serve as a validator node, and if not, how the bank will validate transactions without serving as a node.
    - Description of which blockchains the bank will provide verification services for (both layer 1 and layer 2).
    - Description of whether the bank will participate as signer (in M-N multisig).
    - Description of whether the bank will serve as custodian. If not, identify which entity will serve in that capacity and provide supporting documentation, including any determinations that the bank will not serve as custodian.
2. Description of projected/target clients the bank expects to serve and whether it would provide transaction verification that extends beyond its existing customers.
3. Discussion of why the bank seeks to engage in each activity.
4. Description of process to select which blockchains/crypto-assets the bank would provide services on/for and supporting analysis for those selections.

Technical:

5. End to end transaction flow diagram of each proposed activity, including:
    - A detailed description of the Bank's role in the process.
    - Any other entities involved and their role in the process.
6. Detailed description of b4,b8 role and the services it will provide to the bank, and to bank customers.
7. Detailed description of custody solution infrastructure, architecture, and controls for key generation, storage, and decryption.
8. Details of logical controls, such as multifactor authentication, user access controls, user access monitoring, user access rights, and logging procedures.
9. Detailed description of bank customers' personally identifiable information that will be disclosed to any outside party.
10. Detailed description of fees the bank will receive from any source (e.g., as incentives for validation from third parties and from customers) and what type of compensation the bank expects to receive.

REL0000042358

Operational:

11. Implementation timelines.
12. Project plans.
13. Risk Assessments.
14. Cost benefit analysis, including expected activity volumes, income projections, and any other analysis performed to support the decision to engage in each activity.
15. Due Diligence analysis and associated documents of all critical third parties, including but not limited to b4,b8, subcustodians, and wallet providers.
16. Contracts (including any drafts that the Bank is reviewing or considering).
17. Overview of the contracting process.
18. Any contract analysis performed prior to execution.
19. Legal analyses of permissibility.
20. Bank's analysis of Securities and Exchange Commission Staff Accounting Bulletin 121 and its applicability.
21. Description of how each proposed crypto-asset activity fits into the Bank's strategic plan, the Board's objectives, and actions that would be taken should the activity fail to achieve the objectives.
22. Policies and procedures (including drafts), including those related to internal controls, consumer compliance, Anti-Money Laundering/Countering the Financing of Terrorism, and complaint resolution.
23. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided with respect to each activity.
24. Organizational charts for each activity.
25. Descriptions of anticipated monitoring.
26. Contingency or wind down plans.
27. Internal training materials, including a list of employees that have or will receive training.
28. Insurance coverages for each activity.
29. Plans for the audit function, including the type of audits to be conducted and the required skillsets of the auditors.
30. Parameters regarding the acceptable crypto-assets to be verified.
31. Policies that dictate how many keys and authorizations are required.

Consumer Protection:

32. Customer agreements and disclosures (including template agreements for TPS service), sample account statements, sample transaction receipts, and any other terms and conditions (draft or proposed).
33. Descriptions of any fees that will be charged to customers and how they will be calculated. Also, describe if and how fees are split among the bank and any third parties, such as other key holders.
34. Webpages, mobile app or online banking screens, marketing materials, press releases, internal scripts, educational materials, and any other publicly-distributed information (draft or proposed).

REL0000042358

35. Description of any eligibility criteria for bank customers to use the service.
36. A description of any planned use of multi-escrow arrangements.

REL0000042358