Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Chicago Regional Office
300 South Riverside Plaza, Suite 1700
Chicago, IL 60606
Telephone: (312) 382-7500

[redacted]

February 15, 2023

Board of Directors
[redacted]

Members of the Board:

Thank you for your response to the findings of the April 25, 2022 joint examination. We have reviewed your correspondence, dated October 31, 2022, and as discussed in our briefing on January 18, 2023, there are additional shortcomings that we bring to your attention and ask for your prompt response. The correspondence included a revised risk assessment and fintech vendor request document. While the Board and management have taken steps to address the findings, significant work is still required to fully address the [redacted] related to the bank's crypto-asset service, provided by [redacted]

Crypto-related activities may pose safety and soundness and consumer protection risks to the institution and its customers. The types and levels of risks are dependent on the type of activity, implementation of the activity, and controls designed to mitigate the risks of the activity. Examples of risks that may be present include compliance, legal, operational, third party, and strategic. Facilitating customer crypto-asset trading alongside traditional banking products and services may also present heightened risk to the bank's customers, such as:

- Confusion about the role of the financial institution in the crypto transactions.
- Lack of understanding about the nature and risks associated with crypto-asset products.
- Inability to differentiate between the nondeposit products and traditional banking products, such as deposit accounts.
- Misunderstanding of federal deposit insurance coverage.

BANK CONTRACTUAL RESPONSIBLITIES AND LIABILITES

The bank's contract with [redacted] establishes a range of responsibilities and liabilities on the bank that go beyond providing an interface for the bank's customer to submit buy and sell and orders to [redacted] It is not clear from the bank's documentation and analysis, including the risk assessment, that the bank sufficiently identified and addressed the implications of such responsibilities and liabilities including the following:

- ensuring that instructions to purchase or sell are promptly and accurately transmitted;
- ensuring that end users have "[redacted]";
- holding and transferring funds at settlement;

- settlement failure due to various factors outlined in the contract;
- maintaining security of the settlement account;
- conducting a Customer Identification Program;
- completing transaction monitoring and sanctions screening for the third party;
- providing consumer-facing trade interfaces;
- providing consumer disclosures;
- providing customer service;
- providing complaint monitoring and resolution; and
- being solely and directly liable, and indemnifying the third party, for any and all failures, errors, losses, and deficiencies of any kind with respect to the settlement account.

RISK ASSESSMENT

In general, the risk assessment was limited and lacked analysis and support for ratings assigned to likelihood, impact, inherent risk, control, and residual risk; lacked an overall risk rating; and lacked details and documentation to support that management has implemented adequate controls. Further, the risk assessment did not identify a responsible party for each risk, which is a component of the bank's risk framework, and the risks identified were neither meaningful nor comprehensive.

Your correspondence does not detail how the Board and management used the risk assessment in the bank's overall framework, including how the assessment informed management of the risks and the level and adequacy of risk management practices. This gap in the risk assessment reflects the absence of, and need for, a clear policy governing this activity and oversight responsibilities. While the risk assessment lists some of the inherent risks applicable to the crypto-asset service, management should strengthen the assessment to address the below weaknesses.

Transactional Risks

The transactional risks identified in the risk assessment were limited to "[redacted]" and "[redacted]." The "[redacted]" risk description is limited to the risk that the contract does not adequately cover the termination of the agreement. However, this narrow consideration of this risk does not consider the potential operational risks, financial risks, or consumer risks of a potential exit beyond coverage of contract terms. The "[redacted]" description does not consider any risks related to the contractual terms that establish responsibilities for and potential liabilities of the bank. Furthermore, there are no controls listed for either risk, and no support for the "[redacted]" and "[redacted]" Inherent and Residual Risk determinations.

In addition, the risk assessment did not reflect the bank's role or contractual obligations related to the activity within transactional risk such as the bank's responsibility to ensure that instructions to purchase or sell are promptly and accurately transmitted to [redacted] The risk assessment did not identify or address the risk of the bank's potential inability to provide access or provide accurate information to customers due to technology service provider or [redacted] disruptions, in the event of an exit scenario, or due to market disruptions. The risk assessment also does not address settlement risk such as, being solely and directly liable, and indemnifying the third party, for all failures, errors, losses, and deficiencies of any kind with respect to the settlement account.

Strategic Risk

The strategic risks outlined in the risk assessment are limited to risk from growth, sensitivity to market risk, and impact to examination ratings, which do not fully address strategic risks, such as industry risk and risk from negative public perception. Furthermore, the controls are largely limited to conducting financial analysis, stress scenarios, and regular review at asset/liability committee meetings. While these items listed as controls may assist in assessing risk, they do not clearly provide controls for managing the various risks.

Legal Risk

The risk assessment lists "[redacted]" as a control. However, SOC reports do not assess an entity's compliance with laws and regulations or compliance management frameworks. In addition, the correspondence did not include any new documentation to reflect review of SOC Reports or Reports of Evaluation in the due diligence files. Therefore, the SOC Reports and the Reports of Evaluation's scope and lack of documented review and analysis of the findings call into question the effectiveness of this control. Management should also assess if the service is consistent with applicable laws and regulations.

Operational Risk

The risk assessment raises bankruptcy as a risk; however, the control is limited to stating that audited financials are reviewed periodically, and "[redacted]." However, the bank did not provide an analysis of audited financials of [redacted] and its various affiliates that provide services or a legal analysis to understand the risk of bankruptcy. Further, while completing reference checks and ongoing financial analyses of a vendor is appropriate, it does not serve as a meaningful control to the risk of bankruptcy and the implications of the bankruptcy to this service and to the bank. Lastly, the risk assessment does not address other potential operational risks, such as information security risk, exposure to cyber-attacks, and third party risk.

Financial Risk

The risk assessment does not identify controls and provides no support for the "[redacted]" Inherent and Residual Risk Ratings. Furthermore, the risk assessment does not address or consider the potential financial risk associated with the various bank responsibilities that are listed in the contract as detailed above.

Compliance Risk

Under "[redacted]" risk, management assigned a Residual Risk rating of "[redacted]" based, in part, on a "[redacted]" control rating for management's review of customer-facing materials and disclosures. Examiners concluded that there is a [redacted] risk for customer confusion regarding the nature and risks of the service, including the applicability of FDIC insurance, without more clear and conspicuous disclosure of such risks. Considering the prominence and timing of information presented in the current version of the mobile application disclosures and [redacted] service pages, the aforementioned "[redacted]" Residual Risk rating is not supported.

In addition, the "[redacted]," "[redacted]" and "[redacted]" risks lists ongoing monitoring through the CMS as a control. However, there is no support evidencing that ongoing monitoring specific to the [redacted] service

and these inherent risks has been established or executed. The CMS Program document provided in the management response was updated to include a consideration for providing input on compliance risks surrounding a product, service, or project. This update states that specific controls to mitigate those risks would be documented by the Compliance Team or appropriate business line; however, specific controls to mitigate risks related to the [redacted] service have not been provided in the risk assessment or elsewhere. Therefore, the adequacy of the bank's control for the inherent risks identified cannot be sufficiently evaluated.

VENDOR DUE DILIGENCE

Management submitted an expanded fintech vendor request form that documented vendor due diligence questions and responses along with source documentation to support their review, but there are minimal assessments and support made within the review. The form should not only recite the vendor's business experience and qualifications, financial condition, legal and regulatory compliance, risk management and controls, information security, and operational resiliency, but also fully document and support the due diligence assessment. The form did not include, and due diligence should include, supporting analysis and justification for the following assessments:

- The form states that all members of [redacted] management appear to have adequate qualifications. However, the form does not provide justification to support the assertion that management has adequate experience, expertise, and qualifications to effectively manage the business, such as tenure of the leadership team in crypto assets; depth of expertise in crypto asset trade execution; depth of expertise and knowledge in crypto asset custody, information security, technology development, crypto regulatory environment, relevant bank regulations; and depth of experience in offering a retail crypto asset product.

- The form responds positively to the financial condition question and states that management has reviewed the financial audit performed by [redacted] in [redacted] and the company has offered additional review of unaudited financials upon request. However, the findings of the review are not clear as there is no documented financial analysis. Furthermore, the positive response did not note that [redacted] reported a $[redacted] operating [redacted] in [redacted].

- The form states that information security policies, procedures, and practices are adequate and effectively tested, with a justification that management reviewed the SOC 2 Type II and reviewed policies and procedures provided by [redacted]. However, as noted above, the bank has not provided a copy of these SOC reports and it is not clear that the scope of the SOCs are sufficient for this activity.

- The form's responses to principal ownership, length of time in business, and regulatory oversight of the company do not accurately reflect the entity that the bank is contracting with, the entity's organizational structure, or affiliate services. The form states that [redacted] has been operating since [redacted]; however, [redacted], the entity that the bank contracts with did not exist in [redacted]. The form also states that the regulators

are the [redacted] and the Securities and Exchange Commission; however, [redacted] is not overseen by either agency.

- The form notes that the business continuity and disaster recovery practices of the organization adequately protect the operations of the business. However, the form does not provide justification that management has fully reviewed the business continuity plans and disaster recovery test, including the results of the testing, and how they align with the bank's objectives.

- The form does not provide justification to support that [redacted] disclosures mitigate the risk of customer confusion in a manner that clearly and fully informs customers of the nature and risks associated with these products.

COMPLIANCE MANAGEMENT SYSTEM

Management's response that "the disclosures on the [redacted] platform do not claim or indicate that the service is FDIC insured" is accurate. Nonetheless, the inconsistency and lack of prominence in disclosing the bank's role and the nature and risks of the service throughout the mobile application limits the clear and conspicuous disclosure of information that could assist customers in making fully informed decisions when using the service. For example:

- The bank's mobile banking application main menu screen includes a link where customers enroll for and subsequently access the crypto-asset service. A disclosure at the bottom of the menu screen notes, "[redacted]." However, there is no disclosure noting that the crypto-asset service is offered by [redacted] and that bitcoin is not FDIC insured.

- Bitcoin trade confirmations for each purchase and sale, provided to customers through the mobile application and via email, list [redacted] name and contact information for customer support. While a disclosure at the bottom of the confirmation page states, "[redacted]," without additional disclosure around the nature and risk of the service, the presence of the bank's name on the confirmation page creates the potential for customer confusion surrounding the role of the bank and the lack of protections afforded to this service.

Financial institutions with strong CMS controls to mitigate risks with nondeposit products, such as the [redacted] crypto-asset service, provide consistent, detailed disclosures across all customer-facing screens when such a product is directly embedded in a bank's mobile application banking platform. The risk for customer confusion is especially present within the bank's mobile banking application as customers can access both the [redacted] nondeposit product and bank FDIC-insured deposit products. Strong controls are those that reduce the risk of customer confusion surrounding the nature and risk of any nondeposit product in a manner that fully informs the customers that bitcoin is: 1) not insured by the FDIC, 2) not a deposit or other obligation of, or guaranteed by, the depository institution; or 3) subject to investment risks, including possible loss. The *Interagency Statement on Retail Sales of Nondeposit Investment Products* and *FDIC Part 328 Subpart B* outlines these types of controls to mitigate risk of customer confusion. Providing consistent, detailed disclosures across all forms

and application interface screens may also mitigate the institution's risk of negative public perception that is presented by offering the crypto-asset service.

Providing customers clear, conspicuous, prominent, and timely information about the potential risks related to any product or service offered by, through, or in connection with the bank enhances transparency and reduces the potential for claims relating to misrepresentation and unfair or deceptive practices against the institution. Such information could include a unique acknowledgement page that prominently states that the customer is leaving the area of the mobile application that displays the bank's products and services and entering the area that displays [redacted] products and service and discloses potential risks related to the service in simple plain language statements. Such enhancements to disclosures related to the [redacted] service may assist the bank to reduce the risk of customer misperceptions about FDIC insurance coverage and ensure customers can clearly differentiate between the nature of and risks related to deposit and nondeposit products offered by, through, or in connection with the bank.

BOARD OVERSIGHT

The Board's actions to address the regulatory concerns with the crypto-asset service cited in the April 25, 2022 joint examination are insufficient. As described above, the bank failed to appropriately address the regulatory findings related to the risk assessment, vendor due diligence, and the compliance management system.

Please provide a response to this letter by March 31, 2023. If you have any questions contact FDIC Case Manager [redacted], or [redacted].

Sincerely,
Gregory P. Bottone
Regional Director
Federal Deposit Insurance Corporation

Sincerely,
[redacted]

cc: Federal Reserve Bank of Chicago