FDIC
Federal Deposit Insurance Corporation
25 Jessie Street at Ecker Square, Suite 2300
San Francisco, California 94105

Division of Risk Management Supervision
Division of Depositor and Consumer Protection
San Francisco Regional Office
(415) 546-0160

Sent via secure email

August 10, 2023

Board of Directors
[redacted]

Subject: Crypto-Related Activities Supervisory Feedback Letter (Letter)

Dear Members of the Board:

On March 22, 2022, [redacted] (bank) notified the FDIC of its crypto-related activity proposal via a [redacted]. The FDIC issued Financial Institution Letter (FIL), FIL-16-2022, *Notification of Engaging in Crypto-Related Activities* on April 7, 2022. 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. FIL-16-2022 stated that the FDIC may request that institutions provide information necessary to allow the FDIC to assess the safety and soundness, consumer protection, and financial stability implications of crypto-related activities.

On May 4, 2022, the bank provided notification of its plan, through an arrangement with [redacted] and [redacted], to offer deposit customers the ability to buy, sell, and hold Bitcoin using the [redacted] Bitcoin Trading Platform (the Platform) directly through the bank's online banking services.

On May 31, 2022, the FDIC and the [redacted] started a joint full-scope Safety and Soundness examination. During the examination, on June 15, 2022, bank management met with the examiners, who presented an additional information request list to bank management. The bank also provided a live demonstration of the crypto-related activity that reflected the bank had moved into the test phase and the purchase and sale of Bitcoin through the Platform was available to bank employees. On July 27, 2022, the FDIC sent a letter to the bank's Board of Directors asking them to refrain from expanding the crypto-related activity to bank customers until the FDIC reviewed outstanding concerns related to safety and soundness and consumer protection and provided supervisory feedback to the bank. On September 20, 2022, bank management provided additional documentation and responses in regard to FDIC follow-up questions submitted on August 22, 2022.

We understand that, as discussed, since the completion of our review, [redacted] has determined to terminate the contract; the feedback can help inform the bank's third party risk management practices.

The remainder of this Letter contains supervisory feedback resulting from the FDIC's review of the bank's arrangement with [redacted] and [redacted]. The scope of this review includes an assessment of the information provided by bank management to date related to this proposed crypto-related activity.

BACKGROUND

Crypto-related activities may pose safety and soundness and consumer protection risks to the institution and its customers. The *Joint Statement on Crypto-Asset Risks to Banking Organizations* (Joint Statement), issued by the FDIC, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency on January 3, 2023, may also serve as a useful resource for the Board and management regarding crypto-asset risks. Events of the past year across the crypto-asset sector have been marked by significant volatility and have exposed vulnerabilities in the sector. These events highlight a number of key risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of, including those outlined in the Joint Statement. The types and levels of risks are dependent on the type of activity, implementation of the activity, and controls designed to mitigate the risks. 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, including:

- Confusion about the role of the bank 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; and
- Misunderstanding the applicability of federal deposit insurance coverage.

Part 328, subpart B of the FDIC's Rules and Regulations, titled "False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo," applies to any person, including non-banks, such as crypto-asset companies. (See 12 CFR part 328, subpart B.) Accordingly, the bank should determine if its vendor management policies and procedures effectively manage crypto-related risks, including compliance risks related to part 328, subpart B. In addition, the FDIC's *Advisory to FDIC-Insured Institutions Regarding FDIC Deposit Insurance and Dealings with Crypto Companies*, issued on July 29, 2022, may also serve as a useful resource for the board and management regarding risks and concerns arising from crypto-assets offered by, through, or in connection with, insured depository institutions.

SUPERVISORY FEEDBACK SUMMARY

Given the unique nature and evolving risks associated with the bank's role in offering the Platform alongside existing bank deposit products, management should perform a robust risk assessment, a comprehensive contract review, and rigorous vendor due diligence prior to offering this new service to customers. The Board should ensure appropriate policies and procedures are in place to govern the activity, including ongoing monitoring requirements, appropriate oversight of management and staff responsible for the Platform, and provide approvals with due consideration of necessary assessments and analyses, in accordance with bank governance procedures.

Further, while the bank has some Compliance Management System (CMS) controls in place to evaluate the risks applicable to this crypto-asset service, Board and management did not fully enhance the CMS to sufficiently consider and mitigate consumer compliance risks involved with facilitating customer crypto-asset trading alongside traditional banking products and services. The Board should enhance the CMS to ensure the risks of consumer harm from the crypto-asset service are appropriately identified and mitigated. Failure to enhance the CMS could result in consumer confusion about the nature and risks associated with crypto-assets and result in consumer harm.

RISK MANAGEMENT SUPERVISION

Board Oversight

Increased Board oversight is needed prior to the Platform being fully launched. A [redacted] Policy (Policy) has been drafted but not yet approved by the Board. However, the Board has not established and documented areas such as ongoing monitoring requirements, performance criteria, and reporting needs that will assist with the governance and risk management of this service. In addition, the Board is not fully informed about the potential risks associated with the proposed new service due to weaknesses in the risk assessment and vendor due diligence process. The Board should ensure policies and procedures are sufficient, and that management performs appropriate risk assessments and due diligence in accordance with the policies and procedures. Discussions of the service, including the Board's assessment and approval of the service, review and approval of the risk assessment, vendor due diligence, and contracts should be documented in the Board minutes. Failure to effectively oversee the implementation of the Platform may lead to ineffective controls to oversee both risk and consumer compliance areas.

Policies and Procedures

The draft Policy lacks clarity on several areas that require attention before the Policy is approved.

- The draft Policy does not provide a governing framework, e.g., the coverage and scope of risk assessment, due diligence, contract review, and ongoing monitoring.
- The draft Policy reflects a lack of understanding of the bank's role in conjunction with the contracts with [redacted]. Specific concerns are noted regarding references to Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT), as there are discrepancies between the related [redacted] contracts and draft bank policies. For example:
  - The draft Policy (see [redacted]) states that [redacted] is responsible for AML/Know Your Customer (KYC) transaction screening; however, a [redacted] contract schedule reflects that the bank is responsible, noting that the "[redacted]". These documents create confusion as to the responsible party for KYC.
  - The draft Policy (see [redacted]) states, "[redacted]" However, as noted above, the contract schedule notes that the bank is responsible for transaction screening. Bank management states that there is no tri-party agreement. There are only agreements between [redacted]k and [redacted] and between [redacted] and [redacted] Accordingly, the respective roles and responsibilities of the bank, [redacted], and [redacted] are unclear with respect to AML/KYC.
- The draft Policy also does not reflect or establish guidelines surrounding the bank's responsibilities, such as marketing, customer service, customer complaint process, AML/KYC, settlement, Information Technology (IT) solution, delivering disclosures and agreements, etc.
- The draft Policy (see [redacted]) notes a daily aggregated transaction limit per customer of [redacted], which appears somewhat arbitrary. Bank management indicated that the limit was established primarily based on limits provided by other crypto exchanges. Unsupported transaction limits are not designed to protect customers and the bank from increasing crypto-related activity fraud.
- The draft Policy (see [redacted]) states, "[redacted]." However, the trade confirmation lists [redacted] Bank and includes bank contact information. Because the bank is identified as the designated point of contact for customer service inquiries, bank customers may perceive the bank, as much as [redacted], as the responsible party if issues do arise.

Lastly, the bank's Vendor Management Policy does not provide specifics for this Platform's unique type of activity/service. The Board should review and determine whether the scope of the Vendor Management Policy is sufficient for this activity, and if not, provide additional criteria that must be considered prior to engaging in a relationship with [redacted].

Failure to construct policies and procedures to oversee this Platform could lead to various oversight weaknesses that may go undetected, exposing the bank to increased financial and consumer compliance risk.

Risk Assessments

Management's risk assessment process for the Platform is not comprehensive and should be re-evaluated. Management has developed the following three documents to assess risks related to crypto-asset activities: a Residual Risk Questionnaire; an Inherent Risk Questionnaire; as well as the Crypto Exchange Memorandum used by the Board. While a variety of risks are considered, bank management and the Board should revisit a number of areas to enhance each of the documents.

Inherent/Residual Risk Questionnaires

The questionnaires are not effective at assessing inherent and residual risks and lack the following considerations:

- The questionnaires do not influence the formal risk assessment process.
- The questionnaires do not adequately identify or measure risk using qualitative and quantitative methods.
- The questionnaires lacked analysis on a variety of areas such as legal and contract risk, which are further discussed below.
- The questionnaires have not been assigned any measurable risk levels to the various categories analyzed and lack consideration of any controls or mitigating factors; thus, it is unclear how the level of inherent and residual risk is determined.

For the questionnaires to be effective at identifying, measuring, monitoring, and controlling risks, bank management should assign inherent risk levels, identify mitigating controls, and determine residual risk levels.

Cryptocurrency Exchange Memorandum

The Board reviewed an internally-prepared Cryptocurrency Exchange Memorandum (Memorandum) on November 29, 2021. The Memorandum states that the risks associated with the service include KYC, personally identifiable information, money laundering, custodian, legal, and reputational. However, the Memorandum includes only brief statements summarizing the risks and does not represent a formal risk assessment of the service being considered.

Management should develop a distinct and comprehensive formal risk assessment for this service that includes a detailed and thoroughly documented assessment of all risks and mitigating controls for the Board to understand and evaluate prior to approving the launch of the Program.

Management and the Board did not adequately consider or document the following items during the risk assessment process:

- Third-party contract risk, including potential bank liability arising from the contract, and mitigating controls
- Potential new customer growth as a result of offering this product, associated deposit growth, and potential impact on the bank's capital planning and liquidity risk management
- Potential legal and compliance risks from facilitating customer purchases of a rapidly evolving and highly volatile asset and the risk of customer confusion of the bank's role, as the crypto-assets can only be purchased, sold, or accessed through the bank by a service available through a non-bank, third-party provider
- Potential legal risks related to permissibility. The assessment of legal risk is entirely dependent on [redacted] and does not address the fact that legal permissibility of the activity and application of Federal banking laws and regulations to the Bitcoin Exchange Services has not yet been fully determined.
- Potential risks related to the operations and financial condition of [redacted] and/or related affiliates
- The bankruptcy remoteness of the crypto-assets held in custody for customers by [redacted] and its affiliates
- If management chooses to exit this activity, risks and potential bank liability of winding down and exiting this service

To address the concerns noted above, management must implement a comprehensive risk framework with accompanying controls that provide for an effective risk assessment of this service pursuant to Appendix A to Part 364 of the FDIC Rules and Regulations, *II. Operational and Managerial Standards*. A comprehensive risk assessment would allow management to appropriately identify potential enterprise-wide risks, as well as the risk of consumer harm, which would enable management to ensure that such risks are sufficiently mitigated. The Board must ensure that an appropriate risk assessment framework with accompanying controls are commensurate with the nature of existing and evolving safety and soundness and consumer protection risks specific to crypto-assets.

Information Technology and Information Security (IS) Risk

According to the documents submitted, access to the Platform will be provided through the bank's E-banking platform [redacted]. As a result, authentication controls to access [redacted] would be in place through the bank's E-banking platform. Users would be authenticated through user identifications and passwords that meet the [redacted] standards and parameters. According to Chief Risk Officer [redacted], all data shared from the E-banking platform with [redacted] is encrypted. Although management has considered some IT- and IS-related risks in relation to the bank's arrangement with [redacted], management has not completed a formal information security risk assessment. Management should complete and document this assessment in order to achieve optimal security, provide an analysis of the potential threats and vulnerabilities to the bank's IT

systems, evaluate risks to customer data and privacy, and establish steps to reduce such risks to an acceptable level. Management is also reminded to adhere to internal policies/procedures when granting third parties access to their banking platform.

Vendor Due Diligence

Management's vendor due diligence review analysis of related documents is limited and requires further development. Management has collected various documents on [redacted] including, but not limited to, the following: financial capacity, legal analysis, platform terms and conditions, AML, Office of Foreign Assets Control, consumer protection disclosures/notification procedures and fee structures. However, there is no documentation concerning the bank's analysis of these and other documents, including how these documents influenced the bank's risk assessments.

The Board should ensure that management conducts and documents a thorough analysis of the vendor's business experience and qualifications, current financial condition (specific to legal entities the bank is engaging with, the vendor's affiliates that the bank is relying on, and any financial strength provided by the vendor's parent or related companies), legal and regulatory compliance, risk management and controls, information security, and operational resilience. Moreover, as policy issues continue to change, and given the recent volatility in crypto-assets, the Board should ensure that management periodically monitors the third party and its impact on the bank and customers. Fully assessing and documenting a new vendor will better inform the Board and management of the risks associated with the vendor, the bank's ability to manage and mitigate those risks, and the vendor's ability to provide a service to the bank's customers.

COMPLIANCE MANAGEMENT SYSTEM (CMS)

The risk for customer confusion is especially present due to the Platform, which is a nondeposit product, being accessible to customers only through the bank's existing online banking platforms where FDIC-insured deposit products are also accessible. Management did not sufficiently enhance the CMS to include consumer compliance considerations related to the [redacted] service.

The CMS exhibits certain weakness specific to the oversight of the bank's third-party relationship with [redacted]. Sufficient consumer compliance-related risk assessment, due diligence, and monitoring plans have not been performed or developed. The following section details the consumer protection risks and the weaknesses in the bank's supervision of its third-party relationship with [redacted]

Consumer Compliance Related Risk Assessments

Management's process to assess consumer compliance risks related to the Platform is not comprehensive and should be enhanced. Although management created an inherent risk

questionnaire and a residual risk questionnaire, the questionnaires are very limited in regards to consumer protection risks and do not inform the formal risk assessment.

Management completed an Inherent Risk Questionnaire on the prospective vendor arrangement with [redacted]; but, it does not sufficiently address the types of risk this Platform may present to the bank and its customers. These risks include, for example, consumer confusion about the nature of, and risks associated with, crypto-assets, and the possibility of omissions or inaccurate disclosures that could result in consumer harm. The Inherent Risk Questionnaire asks management to list applicable regulations; however, the list of regulations does not include *Unfair or Deceptive Acts or Practices* under Section 5 of the Federal Trade Commission Act (UDAP), *Electronic Funds Transfer* (Regulation E), or FDIC Part 328 *Advertisement of Membership, False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo* (FDIC Part 328). For example, in assessing potential risks related to Part 328, the bank should consider the restrictions on using the official advertising statement when advertising nondeposit products and the prohibitions against misrepresentations about deposit insurance and the misuse of the FDIC's name or logo, with respect to representations regarding Bitcoin. The Inherent Risk Questionnaire rates the inherent risk of noncompliance as "[redacted]" because exposure may result in nominal fines or non-monetary penalties; but, it does not provide any detail on the types of concerns with the vendor that were contemplated or assessed to reach this conclusion.

The Inherent Risk Questionnaire is accompanied by a Residual Risk Questionnaire that similarly lacks sufficient detail on consumer compliance considerations. The Residual Risk Questionnaire states that the residual compliance risk is "[redacted]," however, it does not include any analysis of mitigating consumer protection controls or supporting details to explain or justify the residual risk rating.

Consumer Protection Due Diligence

The bank's consumer protection due diligence for the new [redacted] service is also insufficient and requires further development. While the bank's consumer protection due diligence included a review of [redacted]'s policies for complaint resolution and advertising controls, management's due diligence did not include sufficient analysis of the disclosures and customer experience when enrolling for and using the Platform. For example, bank management has not sufficiently reviewed the compliance disclosure's communication of the nature and risk of the Platform to assess the risk for customer confusion regarding the bank's role in the crypto-asset transactions.

The Platform's layout and design may contribute to customer confusion. The bank's customers will access the Platform by selecting the "Bitcoin" option from the online banking interface menu, which is listed between multiple deposit-account-related features, such as "Transactions" and "[redacted]" The design similarities and overall placement make the crypto-asset product appear to be another feature of a traditional deposit account. This creates the potential for customer confusion if disclosures do not clearly and conspicuously differentiate the

Platform and Bitcoin from FDIC-insured bank deposit products.

During the enrollment process, customers are presented with information and disclosures surrounding the service prior to being able to buy or sell Bitcoin using an existing bank demand deposit account. During this process, customers are presented with the Bitcoin Trading Platform Terms & Conditions (terms and conditions) and embedded [redacted] E-Sign Consent and Privacy Policy. These terms are shown electronically to customers and include information that the product is not insured by the FDIC and is subject to risk, including possible loss of value. However, there is no disclosure of the risks that Bitcoin balances are not deposits or other obligations of the institution and are not guaranteed by the institution. Further, the bank does not prominently disclose that a customer's access to their crypto-asset account may be suspended by [redacted] This would prevent customers from completing orders or other crypto-related actions on the bank's online banking service, which is the only method that customers can access or submit orders to [redacted] In instances of market turmoil or declining prices, the inability to sell could amplify customer losses.

During the enrollment process, customers are not required to scroll through the entire legal disclosure before accepting the terms and conditions, and are not receiving information about the nature and risks of this product in simple plain language that they must affirmatively acknowledge. Therefore, it is possible for a customer to agree to the terms and conditions without understanding the bank's role and the risks related to nondeposit products.

In the various other electronic pages that the customers are presented with during the enrollment process, and when subsequently accessing the Platform or viewing the Bitcoin Balance through the Bitcoin widget, some information is presented on the nature and risks related to the Platform. The disclosure that states "[redacted]," is consistently presented, but information on the risks related to the Platform is inconsistently presented, and the placement, format, and timing of such language is not always clear and conspicuous. This includes, but is not limited to, the risk of customer confusion that Bitcoin is not insured by the FDIC; not a deposit or other obligation of, or guaranteed by, the depository institution; or subject to risks, including possible loss. The following include some noted examples where the bank did not present clear and conspicuous information on risks of the Platform and suggested measures to consider:

- The "[redacted]" and "[redacted]" pages state or imply information about the potential benefits of Bitcoin without disclosing the potential risks of purchasing this nondeposit product. In additional to information about the potential benefits, the Bank may also wish to consider including information about the risks related to the transaction, which may help minimize customer confusion related to the insured status of the activity.
- The customer acknowledgement page for the various Platform terms and conditions states that [redacted] does not make any recommendations regarding buying or selling of Bitcoin; but, the Platform does not contain any information indicating that the bank is not endorsing or recommending Bitcoin. This may help ensure clear and conspicuous disclosures to consumers regarding the nature and risks associated with these services.

- The confirmation page presented prior to the customer initiating a purchase or sale of Bitcoin does not include any disclosures related to the risks prior to submitting the transaction. The Bank may also wish to consider including information about the risks related to the transaction, which may help minimize customer confusion related to the insured status of the activity.
- The sample transaction receipts, which confirm the purchase or sale of Bitcoin, include the bank's name, logo, and contact information for customer service inquiries; but, the receipts do not disclose any information about the risks related to the transaction. The Bank may also wish to consider including information about the risks related to the transaction, which may help minimize customer confusion related to the insured status of the activity.

Also, certain electronic pages displayed to customers using the Platform use inconsistent terminology from the terms and conditions. The following examples of such inconsistencies further evidence weaknesses in bank management's due diligence review:

- The pages presented to customers during buy and sell transactions show the "[redacted] bitcoin." The term "value" is inconsistent with the terms and conditions, which use the word "price." The terms and conditions define "price" to be inclusive of [redacted]'s calculated market value and added spread, which is presented to customers on the buy/sell pages.
- The Bitcoin Home Page uses the term "Bitcoin Account Value" instead of the term "Balance," which is the term used in the terms and conditions. The distinction is material because "Balance" informs the customer that the displayed dollar amount includes both the pending balance and settled balance.

In addition, the minimum and maximum daily Bitcoin transaction limits are not clearly disclosed in the terms and conditions or other disclosures presented to bank customers. The information provided by bank management states that customers can select any amount between [redacted] when purchasing Bitcoin. The bank's internal procedure, titled Bitcoin Trading Platform Job Aid, states that there is a buy limit of $[redacted] per transaction and a [redacted] daily limit. However, the terms and conditions that are provided to customers only disclose the [redacted] buy limit per transaction.

<u>Ongoing Monitoring of Consumer Protection Risk</u>

The bank's plan for the ongoing monitoring of Bitcoin-related consumer protection risk is insufficient and requires further development. The bank did not provide any information about the scope and frequency of the ongoing monitoring of consumer protection risk for the Bitcoin service. The development and implementation of a risk-based ongoing monitoring program is necessary to ensure consumer protections are effectively managed, including those related to UDAP and FDIC Part 328.

Consumer Protection Supervisory Feedback Summary

The following supervisory feedback will strengthen the bank's CMS and includes measures that may help ensure clear and conspicuous disclosures to consumers regarding the nature and risks associated with the [redacted] crypto-asset service:

- Ensure that sufficient CMS controls are in place to identify, evaluate, and appropriately mitigate the risks of consumer applicable to the crypto-asset service that is offered alongside traditional banking products and services. Failure to implement an enhanced CMS could result in consumer confusion about the nature and risks associated with crypto-assets, including potential consumer harm.
- Consider providing customers with clear and conspicuous disclosure on the nature of, and risks associated with, the platform. The Interagency Statement on Retail Sales of Nondeposit Investment Products (Interagency Statement) may be a useful resource for bank management to enhance the risk assessment process and provide language to customers on the nature and risk associated with the platform in a manner that:
    - Neither misleads, nor confuses, or is likely to mislead, the institution's customers about the role of the institution in facilitating its customers' transactions with crypto-assets provider, [redacted], or the institution's endorsement of such products or services.
    - Minimizes the possibility of customer confusion between the protections afforded to the institution's FDIC-insured deposit accounts and non-insured products.
    - Provides clear and complete information on the possible loss of value associated with the [redacted] service.
- Consider providing customers with a notification when they are leaving the area of the bank's online banking platform that displays bank products and services and are entering an area that displays [redacted] products and services. The bank may wish to consider including a unique acknowledgement page during enrollment, and subsequently when accessing the service, that prominently states that the customer is leaving the area of the online banking platform that displays the bank's products and services and entering the area that displays [redacted] products. This page could include clear warnings about potential risks to the consumer and that the bank does not endorse or recommend the Bitcoin services that customers can access through the bank's online-banking platform. During enrollment, the Bank could consider whether customers be asked to affirmatively acknowledge that they have read and accepted these simple plain language statements regarding the risks as presented.
- Ensure all buy and sell order limits, such as minimum, maximum, and daily, are clearly disclosed to customers and are reflective of actual practices.
- Ensure that the terminology used to communicate with customers is consistent. The terminology should be consistent across the Platform, in Platform-related terms and conditions, or other Platform-related disclosures and communications, including advertisements, customer-facing images, disclosures within the online portal, as well as any oral communication with customers.

- Implement a risk-based ongoing monitoring program that includes a review of consumer protection risks for the [redacted] service. The ongoing monitoring program should enable management to ensure that the crypto-asset services meet all of the bank's consumer protection responsibilities, including those related to UDAP and FDIC Part 328. Management should develop and implement procedures to monitor [redacted] platform updates and changes to [redacted]'s service offerings, including disclosures, terms and conditions, transaction limits promotions and bonuses, and any other customer facing materials that could create customer confusion or customer harm prior to implementation and periodically thereafter.
- Consider providing additional warnings that further clarify other risks involved in using the Platform, such as that [redacted] may suspend customer access to the service and prevent customers from completing orders or other crypto-related actions on the bank's application.

MEETING WITH BANK MANAGEMENT

Examiners met with bank management on August 4, 2023 to discuss a number of the findings disclosed in this letter. Representing the FDIC was Case Manager [redacted], Consumer Compliance Technology Specialist [redacted], Senior Examiner [redacted], and Supervisory Examiner [redacted]. Representing the bank was Chief Financial Officer [redacted], Head of Digital Banking [redacted], Chief Risk Officer (CRO) [redacted] and General Counsel [redacted]. Representing the [redacted] was Portfolio Manager [redacted].

During the meeting, management was receptive to the findings and noted that at this point a crypto-related activity proposal was not being considered by the bank. CRO [redacted] noted that the regulators might not have had the whole picture of the bank's review process, as examiners only reviewed a segment of the bank's material. CRO [redacted] said that, as requested, a formal response to the Letter from the Board would be provided to the FDIC.

CONFIDENTIAL NOTICE

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). Please notify the FDIC immediately if you receive a subpoena or other legal processing calling for the production of this letter or a description of its content.

ACTION REQUESTED

Given the status of the [redacted] initiative, we request the Board review this Letter at their next meeting, document their review in the minutes, notify us of any material changes in the status of the program, and provide a written response within 45 days of receipt of this Letter. If you have any questions, please contact RMS Assistant Regional Director Jaclyn V. Valderrama at [redacted], RMS Case Manager [redacted] at [redacted], DCP Assistant Regional Director Matthew Sheeren at [redacted], or DCP Compliance Technology Specialist [redacted] at [redacted]. Written correspondence should be addressed to my attention at the San Francisco Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (https://securemail.fdic.gov) using the following e-mail address: SFMailroom@FDIC.gov. Information on how to use secure email and FAQs about the service can be found at https://www.fdic.gov/secureemail/.

Sincerely,

/s/Kathy L. Moe

Kathy L. Moe
Regional Director