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 14, 2023

Board of Directors
[redacted]

Subject: Crypto-Asset Activity Review Supervisory Feedback Letter (Letter)

Dear Members of the Board:

On June 30, 2021, [redacted] engaged in a Statement of Work (SOW) with its core service provider, [redacted], to develop a crypto-asset service offering with third party provider [redacted]. [redacted] is a subsidiary of [redacted] (collectively, with affiliates and subsidiaries, referred to as [redacted]). The SOW is focused on [redacted] building a technology solution directly with [redacted]'s application program interfaces (APIs) that would ultimately allow [redacted]'s online deposit account customers the ability to buy, sell, and hold an ownership interest in bitcoin using the [redacted] Bitcoin Trading Platform (Platform). The Bank continues to evaluate the Platform and has conducted beta testing by Bank employees.

On April 7, 2022, the FDIC issued Financial Institution Letter (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. An initial discussion on the Platform was held between the FDIC and Bank management in May 2021 followed by several subsequent discussions beginning in April 2022. As stated in FIL-16-2022, 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. In order to begin those assessments, in April and October of 2022, the FDIC requested additional documentation from the Bank, including policies, processes, and controls established and maintained in relation to this crypto-related activity. This Letter provides supervisory feedback relative to the consumer protection and risk management considerations of the proposed crypto-related activity.

Since the completion of our review, [redacted] issued a Notice of Termination electing to terminate the existing agreement with [redacted]. In its correspondence to the Bank, [redacted] indicated that they will communicate specific timing and details of winding down the service, and it is our understanding that the Board will be voting on winding down the [redacted] initiative at the upcoming August 29, 2023 Board meeting. Despite the likely and eventual wind down of the

[redacted] initiative, we are issuing this feedback letter to help inform the Bank's third party risk management practices.

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 on January 3, 2023 by the FDIC, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency, may serve as a useful resource for the Board and management regarding crypto-asset risks. Recent events 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 risks. Examples of risks that may be present include, but are not limited to, 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 crypto transactions;
- Lack of understanding about the nature and risks associated with crypto-asset products;
- Inability to differentiate between 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 third-party risk 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, through FIL-35-2022, 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

While management is commended for taking numerous actions, such as developing policies, progress reports, and testing requirements, a number of risks have either not been fully assessed or have not been fully reviewed based on risk assessment findings. Other weaknesses include limited due diligence processes and a Digital Asset Policy that does not establish meaningful

standards, processes, or controls, as well as financial projections that lack supportable assumptions. While the Bank has some Compliance Management System (CMS) controls in place to evaluate the risks applicable to the Platform, the 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.

Given the unique nature and evolving risks associated with the Bank's role in offering products that are not FDIC-insured through the Platform alongside existing FDIC-insured 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 and appropriate oversight of management and staff responsible for the Platform, and provide approvals with due consideration of necessary assessments and analysis, in accordance with Bank governance procedures. In addition, the Board should enhance the CMS to ensure the risks of consumer harm from the Platform 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.

DETAILED FINDINGS AND FEEDBACK

Risk Assessments and Vendor Due Diligence

Management outsourced almost all of the risk assessment and due diligence processes to [redacted] and [redacted]. Management noted that external parties were engaged to help bolster staff knowledge and provide an external perspective. This decision was also influenced by management indicating that their knowledge of crypto-assets was more focused on consumer risks rather than institutional risks for onboarding this type of product.

While management has since broadened their knowledge around crypto-assets and hired additional staff with specific crypto-related skillsets, as described below, a number of risk assessment and due diligence areas were not fully reviewed. In addition, management has not implemented a formal process to track or monitor findings and recommendations from these external reports, which need to be developed going forward. Lastly, while management noted that their due diligence prior to selecting the firms was based on conversations as well as past engagements, no formal documentation was retained to demonstrate the external parties' experience with this novel arrangement. The following concerns are noted with the risk assessment and due diligence process.

[redacted] *Risk Assessment*

[redacted] performed a risk assessment that evaluated traditional banking areas such as liquidity risk, market risk, compliance risk, and Anti-Money Laundering/Countering the Financing of

Terrorism (AML/CFT) risk. While [redacted] provided a narrative regarding each of the rating factors, a rating scale or detailed narrative to support the final conclusion was not included or described. Furthermore, residual risk areas lacked specific or actionable details that management could initiate to further reduce the level of risk exposure. Examples (not all inclusive), of areas with limited or inaccurate information to support an overall rating are as follows:

- Liquidity Risk: Both inherent and residual liquidity risk were identified as low; however, multiple references of liquidity reports performed by the Bank with crypto-asset assumptions were not located. This includes reviews by treasury management, a third party risk review, and liquidity risk modeling reports.
- Market Risk: Both inherent and residual market risk were identified as low; however, no consideration is given to potential volume impacts that could not only arise from price volatility but also from macroeconomic factors.
- Credit Risk: Several risk mitigants outlined for credit risk are inaccurate or not supported:
  - [redacted] was not operating at the time the risk assessments were completed, and there was no look-back or updated review of [redacted]'s financial condition once the Bank contracted with the entity. The financial analysis was of the consolidated [redacted] entity, without analysis of [redacted] or its potential reliance on the strength of its parent or other affiliates for support. This is particularly relevant as the Vendor Financial Review reports negative cash flow and high leverage. To fully inform management and the Board, the risk assessment should acknowledge that the entity had not been established and had no financial condition to assess, which would allow the Bank to determine appropriate controls, as applicable.
  - The risk assessment indicates that oversight provided by the [redacted] is a mitigating factor for credit risk. However, while [redacted] affiliates have certain [redacted] from [redacted], [redacted] is not overseen by [redacted]. Furthermore, it is not clear how oversight by [redacted] is a mitigating factor for credit risk, which is also listed as a mitigant for operational, compliance, and reputation risk.
  - "[redacted]" is noted as a mitigating factor. However, neither [redacted] nor its parent hold a trust charter.
- Compliance Risk:
  - "[redacted]" of the risk assessment
    - States, "[redacted]." However, as noted above, [redacted] is not an [redacted]-regulated entity. The August 2020 BSA/AML audit reviewed by [redacted] does not clearly reflect that [redacted] was included in the scope of the audit. [redacted] was not formed until March 2021, well after the audit was performed.
    - Outlined that the Bank's transaction monitoring system cannot identify transactions and that improvements are needed prior to launch. The

October 2022 Project Rollout Plan reflects that testing of the transaction monitoring system was in progress. It is not clear whether necessary improvements have been implemented.

- "[redacted]" of the risk assessment
  - States that the Bank and [redacted] agree to mitigate consumer confusion by providing clear disclosures around fees "[redacted]" However, no other Bank-developed disclosures were provided for review.
  - Does not identify potential non-compliance with Part 328 of the FDIC's Rules and Regulations as a consumer protection compliance risk. 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.

[redacted]'s risk assessment also did not include assessments on various key risk areas such as settlement, third party, contract, marketing, ownership, legal, affiliate, and pricing/spread. The risk assessment also does not reflect implications of various contractual responsibilities and liability, including the following:

- ensuring that instructions to purchase or sell are promptly and accurately transmitted;
- ensuring that end users have "good funds";
- holding and transferring funds at settlement;
- being liable for the amount of [redacted]'s net losses incurred due to settlement failure;
- maintaining security of the settlement account;
- conducting a Customer Identification Program;
- completing transaction monitoring and sanctions screening for [redacted];
- providing consumer-facing trade interfaces;
- delivering [redacted] customer disclosures;
- providing customer service; and
- performing complaint monitoring and resolution.

Management should ensure an appropriate risk assessment incorporates an enterprise-wide focus of the activity, entity, contractual obligations, and controls. Given the novel nature of the proposed activity, risk assessments should incorporate areas that demonstrate a complete understanding of the resulting arrangement. Such reviews should ensure information in the risk assessment is accurate with mitigating controls. In addition, management should document due diligence performed on external firms to ensure a company has the experience and wherewithal to appropriately assess a product. Failure to conduct appropriate risk assessments and due diligence reviews could lead to undetected risks, or the inability to establish mitigating controls, outside the Board's risk appetite.

[redacted] *Due Diligence*

[redacted] performed the vendor due diligence assessments on areas such as [redacted]'s cold storage system and organization controls (SOC) reports, financials, reputation, information security and privacy, and business resilience. Each report includes information on what was reviewed as well as a final assessment on the area. The following concerns are reflective of a lack of support for certain ratings by [redacted]:

- The financial review rated [redacted] and its subsidiaries as adequate, despite [redacted] net losses and high leverage [redacted] The review document does not outline which metrics are reflective of an 'adequate' versus 'watchlist' rating, the latter of which is defined as "financial concerns noted warrant ongoing monitoring." Given these factors, an 'adequate' rating lacks support.
- The information security and privacy risk review lists a series of items, such as whether certain programs (such as information security, incident response, vendor risk management) are in place and a high level list of the security protocols and controls are established. However, the review does not address, analyze, or document whether the information security, incident response, and vendor risk management programs or the controls are appropriate, and instead lists page numbers of 'source reference' which appear to be the SOC reports. However, the SOC reports are limited to a review of the cold storage solution.
- The cybersecurity review outlines whether a number of practices are in place, but is limited to listing the page number of the 'source reference' document. The review does not document the adequacy of those practices and relies primarily on the SOC reports, which are limited to the cold storage solution, and on [redacted]'s Compliance Manual.
- The review does not assess key [redacted] operational functions beyond information security, privacy, and resilience, such as the information technology solution interfacing with the Bank and consumers, transactional functions, recordkeeping functions, or settlement functions, which may introduce both operational and transaction risk.

Furthermore, management has not formally tracked or addressed any of the findings. For example, multiple assessments indicated that certain areas could either not be assessed by [redacted] or that additional follow-up was necessary. Management did not track, follow-up, or monitor these findings. Examples include, but are not limited to:

- If [redacted]'s source code is deposited in escrow to allow a client to continue the service if the vendor is no longer able to.
- If business continuity tests at [redacted] are communicated with the Bank.
- If client data is segregated at [redacted] from their other clients.

In addition, [redacted]' due diligence related to cold storage identified various areas "[redacted]." Those include specific segments such as physical security, data security, and data breach management. While these areas do not necessarily mean there is a

concern with [redacted], [redacted] or their related entities, management has not further assessed these unconfirmed segments. In addition, the cold storage risk assessment includes a variety of carve outs from third party vendors.

Management should ensure appropriate due diligence is performed. This includes reassessing the various findings within [redacted]' review, including certain controls that did not operate, as well as areas that were unconfirmed. Management and the Board should ensure processes, policies, and guidelines are in place to ensure appropriate review and oversight of due diligence is performed to assess the adequacy of the analysis before it is presented to relevant committees and the Board. Failure to do so could lead to risks to the Bank and its customers.

Crypto-Asset Policy

The Bank's Digital Asset Policy (Policy) should be updated to reflect various aspects of the current program. The Policy (Board approved March 2022) identifies a number of key areas such as definitions, delegations of responsibility, and training. However, the Policy does not provide a clear framework of expectations related to the program, such as:

- The required scope of risk assessments, due diligence reports, contract review procedures, or ongoing monitoring practices.
- The Bank's responsibilities to [redacted] (such as delivering disclosures and agreements, marketing, customer service, complaint management, BSA/AML/CIP, and settlement).
- The Bank's expectations and processes for areas such as monitoring, testing, control failures/issues, or remediation requirements.
- The Bank's administration and oversight of the omnibus account used to confirm crypto assets purchased by customers actually exist.

Failure to maintain adequate policies and procedures for management to follow could lead to operational disconnects and unenforced controls, which in turn could expose the Bank to various levels of risk or consumer harm.

Third Party Risk

While efforts have been made to understand third party risks associated with both [redacted] and [redacted], additional clarity is needed to evaluate the potential exposure to the Bank. Specifically, management has not yet received a full list of third parties (fourth parties to the Bank) that [redacted] uses to perform various operations. In addition, four sub-servicers/fourth parties that were identified within the SOC reports were not followed-up on by management. Lastly, the Bank's contract with [redacted] indicates that [redacted]'s features will be provided by APIs and "[redacted]" Bank management has not obtained a list nor assessed what those solutions are and if any risk is present.

At a minimum, management should understand the third and fourth parties involved, the risks that the parties and their products and services present, and assess how each party, product, or service may introduce risk to the Bank. Then, management can begin to determine how to assess

the related risks with applicable parties, including the identification of inherent risks, controls, and residual risks. Proactive third party oversight will help mitigate undetected risk with third party partners.

Financial Projections

financial projections that incorporate expected users' adoption with need attention. As noted briefly above, due diligence documents noted that management incorporated liquidity projections in various internal liquidity reports; however, no projections were located. Management should revisit liquidity projections to understand the potential impacts that may result from onboarding this product to the Bank's end users. Onboarding new services without properly projecting funding requirements could result in unanticipated liquidity needs.

In addition, revenue projections lack certain critical assumptions from the Bank. Financial projections provided to the Board focus on establishing a break-even point for the Platform generated from fee income, as well as revenue volumes over the next five years. While these metrics gave the Board a sense of expectations during the initial due diligence phase, some of these customer expectations were generated from and included little to no support. Furthermore, those projections were likely generated when bitcoin prices were rapidly appreciating in comparison to the US Dollar and did not consider any type of range or pullback in the market. Management should revisit the report and consider a range of results that incorporate different levels of adoption and transaction volume. If properly constructed, revised figures should allow the Board to understand various revenue scenarios that must be considered during the implementation process.

Prepaid Asset

As of March 2022, the Bank accrued approximately $ in expenses related to the design and buildout of the Platform. At that time, the Bank began amortizing an expense of $

Compliance Management System

The risk for customer confusion is heightened due to the Platform, which is a nondeposit product, that is only accessible to customers through the Bank's existing online banking and mobile application (app) platforms where FDIC-insured deposit products are also accessible. Management did not sufficiently enhance the CMS to identify and mitigate consumer compliance considerations related to this crypto-asset service. In addition, the following section details weaknesses in the evaluation and controls of consumer protection risks conducted by the Bank of its third-party relationship with Addressing the items below will help ensure that CMS controls are in place to evaluate and monitor the risks applicable to this service, and

could assist to mitigate the consumer compliance risks involved with facilitating bitcoin trading alongside traditional banking products and services.

Website and/or Mobile Application and Disclosures

Bank customers will access the Platform by selecting the "bitcoin" option from the online banking or mobile app interface menu, which is listed between multiple deposit account-related features such as "Accounts" and "[redacted]." During the online or mobile app 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. Key risks include customers not understanding the distinctions between FDIC-insured bank deposit products and the Platform and bitcoin when enrolling in the Platform.

During this process, customers are presented with the [redacted], which contains the embedded [redacted] End User Agreement (EUA or Terms and Conditions), [redacted] E-Sign Consent, and Privacy Policy. This page also includes a statement that "[redacted]." However, customers have not been provided information that states bitcoin constitutes one of the types of products. This page could clearly state that these are 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 Program. Further, there is a statement that "This Product is not insured by the FDIC or SIPC." However, while accurate that crypto-assets are not insured by the FDIC, "This Product" has not been defined in any of the Terms and Conditions. In addition, deposit insurance protections provided to depositors by the FDIC is different from the investor protections provided by the Securities Investor Protection Corporation (SIPC). The disclosures and disclaimers could more clearly distinguish what protections are not afforded to crypto-assets. For example, by using terminologies such as, not insured by the FDIC and not protected by the SIPC, the disclosures could more clearly distinguish such protections.

The *Interagency Statement on Retail Sales of Nondeposit Investment Products* (NDIP Statement) may serve as a useful resource for Bank management to consider the nature and risks associated with the Platform including, but are not limited to, that bitcoin is: 1) not insured by the FDIC, 2) not a deposit or other obligations of, or guaranteed by, the depository institution, or 3) subject to investment risks, including possible loss. While some information is presented on the nature and risks related to the Platform, information on the risks is inconsistently presented and the placement, format, and timing of such language is not always clear and conspicuous. In addition, there are differences in how such information is presented across the online banking and mobile app versions of the Platform. For example:

- The embedded Terms and Conditions that customers must acknowledge electronically include information that the product is not insured by the FDIC and is subject to risk, including possible loss of value. To further help minimize consumer confusion and harm, the Bank could consider whether to also inform customers that Bitcoin balances are

not deposits or other obligations of the institution and are not guaranteed by the institution.

- The "Confirm Trade" buy and sell pop-up presented prior to the customer confirming a purchase or sale of Bitcoin through the online banking platform does not include disclosures related to the risks prior to submitting the transaction. These same confirmation pages in the mobile application do clearly state: 1) Bitcoin accounts & services by 2) Not FDIC insured, 3) Not a deposit, and 4) May lose value at the bottom of the screen.
- The transaction receipts that confirmed the purchase or sale of Bitcoin include the Bank's name, logo, and contact information for customer service inquiries. The transaction confirmation does not disclose any information about the risks related to the transaction but the online banking page footnote included on all Platform pages states: 1) Bitcoin accounts and services provided by 2) Bitcoin is not a security and s not an SEC-registered exchange, 3) Bitcoin balances in our Account are not insured by the FDIC or SIPC, and 4) There are risk associated with bitcoin trading, including possible loss of value. The footnote disclosures for all mobile application pages, including transaction receipts, include a slightly different disclosure that states: 1) Bitcoin accounts & services by 2) Not FDIC insured, 3) Not a deposit, and 4) May lose value.

To help ensure clear and conspicuous disclosure regarding the nature and risks associated with the Platform, the Bank could consider adding a unique page or specific checkbox separate from existing pages or disclosures. As suggested in the NDIP Statement, this could be in the form of simple plain language statements regarding the risks presented that requires customer acknowledgement prior to enrolling for the Platform. The Bank may also wish to consider providing additional disclosures on subsequent pages that further clarify the risks involved with this service, including that may suspend Bank customer access to the service and prevent customers from completing other actions on the Platform. Additionally, to further ensure customers understand the nature and risks associated with the Platform, the Bank could consider requiring that the various disclosures be opened by the customer before they can provide an affirmative response that they have read and agree to terms and conditions of the service, which is not currently required.

While various information is presented across the online banking platform and mobile app on 's role in offering the service, it may not be clear to the Bank's customers when they are leaving an area that provides bank deposit products versus services for products and services. The Bank may wish to consider adding a message or page after a customer clicks "Sign Up" to indicate that the customer is leaving an area of the Bank that offers banking products and services, and entering an area offering services, which may help ensure customers better understand the distinction.

Furthermore, on the Bitcoin Account Summary page, customers are presented with a Bitcoin price that shows the "Market Value" for information purposes; however, there is no disclosure or information provided that states where that value is derived from. To ensure that customers

clearly understand that this is different than the "Price" for a bitcoin charged by , consider adding the source of the market value (e.g. "" or other index). On the same page, the amount of bitcoin held by a customer is listed under "Bitcoin Holdings" whereas the EUA reflects "" and "Bitcoin Balance." Lastly, the online banking and mobile app "Confirm Trade" buy and sell pages show a transaction fee of percent; however the EUA states there is a . Management should ensure that all fees, terms, and conditions, and other relevant terminology are complete and consistent between the EUA, the online banking pages, mobile application, and any other Bank policies, procedures, or call center scripts.

Monitoring and On-going Vendor Due Diligence

Management should develop and implement procedures to monitor and platform updates and changes to 's service offerings, including promotions and bonuses, prior to implementation and periodically thereafter. Also, consider implementing a mechanism to identify customer confusion, and the need to mitigate or adjust disclosure practices if needed. This could be accomplished through routine review of customer complaints and inquiries on the program. Lastly, the compliance risk assessment should be updated to include the consumer compliance risks associated with offering crypto-asset related products and services.

Failure to maintain a sufficient CMS could result in customer confusion about the nature and risks associated with crypto-assets, including potential consumer harm. Again, the *NDIP Statement* may serve as a useful resource for Bank management to enhance the risk assessment process and ensure clear and conspicuous language is provided to customers 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, , or the institution's endorsement of such products or services.
- Minimize the possibility of customer confusion between the protections afforded to the institution's FDIC-insured deposit accounts and non-insured products.
- Provide clear and complete information on the possible loss of value associated with the service.

Meeting with Bank Management

Examiners met with Bank management on July 11, 2023 to discuss a number of the findings disclosed in this letter. Representing the FDIC was Examiner-in-Charge , Financial Analytics Data Scientist and Compliance Technology Specialist . Representing the Bank was Director of Digital Channels , Product Manager , Chief Banking Officer , Chief Operating Officer , Regulatory Liaison , Director of Community Development and CRA Officer , and Chief Risk Officer During the meeting, management was receptive to the findings and noted that a discussion would commence with senior

management and the Board regarding next steps with the program. Management noted that a formal response would be provided following those discussions.

Later that day, Bank management informed the FDIC that [redacted] sent correspondence to the Bank indicating that [redacted] is electing to terminate their agreement with the Bank effective immediately [redacted] Bank management also noted that [redacted] has also terminated their agreement with [redacted] related to the Bitcoin Service.

Confidentiality 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 current status of the [redacted] initiative, we request that 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 project, 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 Valderrama at [redacted], RMS Case Manager [redacted] at [redacted] DCP Assistant Regional Director [redacted] at [redacted], or DCP Review Examiner [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