Division of Risk Management Supervision Division of Depositor and Consumer Protection **MEMORANDUM SYSTEM**	Classification Number: 6600 Date: June 06, 2022 Issuing Office: RMS and DCP Contact: RMS: [redacted] DCP: [redacted] ☐Notice ☒Memorandum

Transmittal No. 2022-014-RMS
2022-003-DCP

Amended 2/8/2024 to include feedback timeframes and instructions to clarify completion of review. Substantive edits in bold.

Amended 10/31/2022 to include a timeframe for initiating consultations, add certain templates, update out-of-scope activities, and incorporate regional office feedback.

MEMORANDUM TO: Regional Directors

FROM: Doreen R. Eberley
Director, Division of Risk Management Supervision (RMS)

Mark Pearce
Director, Division of Depositor and Consumer Protection (DCP)

SUBJECT: Procedures for Reviewing Notifications of Engagement in Crypto-Related Activities

1. **Purpose:** To establish procedures for receiving, reviewing, and responding to notifications from FDIC-supervised financial institutions engaged in or considering engaging in crypto-related activities, pursuant to Financial Institution Letter (FIL) 16-2022, "*Notification of Engaging in Crypto-Related Activities*" (issued April 7, 2022).

2. **Background:** FIL-16-2022 requests 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) notify the appropriate FDIC Regional Director and provide all necessary information that would allow the FDIC to assess the safety and soundness, consumer protection, and financial

stability implications of such activities. The FDIC will review the relevant information and provide supervisory feedback to the institution, as appropriate.

The FIL describes crypto-related activities as follows: "By "crypto-asset," the FDIC refers generally to any digital asset implemented using cryptographic techniques. The term of "crypto-related activities," for the purposes of this FIL includes acting as crypto-asset custodians; maintaining stablecoin reserves; issuing crypto and other digital assets; acting as market makers or exchange or redemption agents; participating in blockchain- and distributed ledger-based settlement or payment systems, including performing node functions; as well as related activities such as finder activities and lending. This listing is based on known existing or proposed crypto-related activities engaged in by FDIC-supervised institutions, but given the changing nature of this area, other activities may emerge that fall within the scope of this FIL. The inclusion of an activity within this listing should not be interpreted to mean that the activity is permissible for FDIC-supervised institutions."

Note that the request applies to activity planned or engaged in by institutions, not their customers. Therefore, crypto-related activity does not include providing deposit account services to crypto-asset automatic teller machine operators, providing deposit accounts used for the business operations of, or processing ACH payments for, crypto-related companies in which the bank does not hold/maintain the funds of the crypto-related companies' customers, or making loans to crypto-asset companies not collateralized by crypto-assets. However, crypto-related activity does include lending when crypto-assets are used or relied upon as collateral and, as noted above, it does include deposit accounts used to maintain stablecoin reserves.

The FIL indicates that crypto-related activities may pose significant safety and soundness and consumer protection risks, as well as financial stability concerns. Moreover, these risks and concerns are evolving as crypto-related activities are not yet fully understood. Note that the notification described in the FIL is not a requirement. However, pursuant to Section 39 of the Federal Deposit Insurance (FDI) Act, Part 364 of the FDIC's Rules and Regulations (including Appendices A and B), establishes safety and soundness standards for all FDIC-supervised institutions. As such, FDIC-supervised institutions should be able to demonstrate their ability to conduct crypto-related activities in a safe and sound manner. This FIL does not address the permissibility of any specific crypto-related activity that an FDIC-supervised institution may engage in under Section 24 or Section 28 of the FDI Act or under Part 362 of the FDIC's Rules and Regulations. Questions concerning permissibility should follow the procedures under Parts 303 and 362 of the FDIC Rules and Regulations.

The FDIC is aware of a number of institutions already engaging in crypto-related activities through previous contacts, press reports, and examination activities, but issued the FIL to help close a gap in data regarding this information. In practice, supervised institutions previously have informed the FDIC of their intentions to engage in crypto-related activities in a variety of ways, including emailing correspondence to a field or regional point of contact, sharing information during examination discussions and interim contacts, and including the information in other correspondence sent to the FDIC.

The FIL describes that the initial notification to the FDIC Regional Director should describe the activity in detail and provide the institution's proposed timeline for engaging in the activity. As notifications are received, the FDIC will review the relevant information submitted by the FDIC-supervised institution related to crypto-related activities and provide appropriate and timely supervisory feedback to the institution. Such information may affect the scope and timing of examination or visitation activities, depending on various factors associated with the crypto-related activities and the institution's proposed timeline.

3. Actions:

a. All RMS and DCP staff should read FIL-16-2022.

b. FDIC staff who receive information about a bank engaged in or intending to engage in crypto-related activity should immediately inform the assigned Case Manager or Review Examiner. Subsequently, the Case Manager or Review Examiner should determine whether or not notification has been provided to the Regional Director.

c. Regional staff should implement the following procedures when an FDIC-supervised institution notifies the appropriate Regional Director that it is already engaged in, or intends to engage in, crypto-related activities, as outlined by the FIL. Regional staff should also implement the following procedures for planned or existing crypto-related activities about which they are currently aware or become aware through means other than notification to the FDIC Regional Director.

i. Tracking System Entry / Update

Immediately upon receiving notification from an institution, or information through any means other than notification from an institution, the Case Manager should create an entry for the institution in [redacted] (tracking system) and complete data fields based on available information. The Case Manager should continue to complete any remaining data fields as the review and feedback processes are completed. If information regarding the institution's crypto-related activities exists in the tracking system, the Case Manager should review the information in the tracking system to ensure it reflects the most current information regarding the activity described in the institution's notification. Initial notifications and follow-up correspondence to or from the institution should be filed in the Correspondence folder in the [redacted].

ii. Review of Initial Notification and Determination of Next Steps

The Case Manager and Review Examiner (or other designated DCP regional point of contact) should review (in consultation with the Washington Office (WO), as discussed below) the initial notification and information received from the institution to determine whether the information received provides a sufficiently detailed description of the activity and whether additional information is needed to assess the safety and soundness, consumer protection,

and financial stability implications. The information needed to make these assessments will vary on a case-specific basis depending on the type of crypto-related activity. Notification from an institution should include a proposed timeline for implementation of the activity or sufficiently detail the history of implementation when already engaged in such activities.

Within ten business days of receiving a notification, and before contacting the institution, the Region should initiate concurrent consultations with RMS and DCP in the WO. WO staff may reach out to the Region prior to that if information is needed. For RMS, initiate consultation with the [redacted] For DCP, initiate an informal WO consultation following existing procedures, including seeking advice from the [redacted], and proceed under the "[redacted]. Also, the Case Manager and Review Examiner (or other designated DCP regional point of contact) should coordinate with the appropriate Regional Counsel (who will consult with WO Legal) on any questions concerning the activity's permissibility and other legal issues to determine whether additional information or documents should be included in the request.

Requests for additional information from the institution should generally be sent within 60 days of notification and should request responses within a specific timeline. After the institution provides responses, subsequent information may be requested if additional detail on an activity is necessary to complete the safety and soundness and consumer protection considerations review. **When the Regional Office, in consultation with the WO, determines that the information provided is substantially complete to perform the review, the Regional Office, in consultation with the WO, should establish and communicate to the institution the expected timeframe in which the FDIC intends to provide supervisory feedback to the institution. Projected timeframes should take into account the complexity of the proposal, the materiality of the proposal's potential implications, as well as any considerations related to the broader supervisory strategy for the institution, both safety and soundness and consumer protection.**

October 2022 Amendment: As a result of the experience gained and collaboration between the Regions and WO on reviews of crypto-related activities to date, template information request lists have been developed for facilitation of customer purchase and sale of crypto-assets through an institution with a third party and crypto-asset collateralized lending. Additionally, a template letter has been developed to notify institutions when their activity has been deemed to be out of scope. These templates have been developed to promote consistency in the communications and information requests sent to institutions nationwide regarding those activities.

As noted above, this update also communicates that the following activities are out of scope: (1) providing deposit account services to crypto-asset automated teller machine operators; (2) loans to crypto-related entities that are not collateralized by crypto; and (3) deposit accounts used for the business operations of, or processing ACH payments for, crypto-related companies in which the bank does not hold/maintain the funds of the crypto-

related companies' customers. RMS and DCP will continue to periodically update this memorandum with activities that have been determined to be outside the scope of FIL-16-2022. For other activities, the decision regarding whether a notification is in or out of scope requires consultation with and concurrence by RMS and DCP in the WO.

Impact to Region/WO Collaboration When Regions Use Templates Without Material Revisions:

- To the extent the Regions receive notifications regarding activities outlined as out of scope in this memorandum, Regions may send a letter to the bank using the attached template without consulting with the WO and without WO review of the letter.
- For other activities deemed to be out of scope after consultation with and concurrence by the WO (as discussed above), Regions may also use the template letter to communicate the decision without WO review of the letter.
- When using the template request lists, WO review is not required prior to sending to an institution. However, the use of the template request lists does not eliminate the requirement to initiate concurrent consultation with RMS, DCP, and Legal upon receipt of a notification and before contacting an institution. This includes coordinating on a cover letter, as appropriate.

When notification from an institution has not yet been provided, but the Region is aware that an institution is already engaged in, or intends to engage in, crypto-related activities, the Region should initiate collaboration with RMS and DCP in the WO to determine next steps, if any, such as contacting the institution and requesting additional information. For RMS, contact the [redacted]. For DCP, contact the [redacted], who will provide guidance as to whether an informal WO consultation is needed.

iii. Safety and Soundness and Consumer Protection Considerations Review

Once additional information is received from the institution, the Case Manager, Review Examiner (or other designated DCP regional point of contact), or examination team (in the case of a visitation or examination) should assess the safety and soundness (particularly in the context of Part 364 and its appendices) and consumer protection considerations related to the activity. Safety and soundness and consumer protection considerations often depend on the facts and circumstances of an institution's crypto-related activity and implementation, and may include, but are not limited to, the following:

Safety and Soundness:

- Asset Quality / Credit Risk Management and Exposure
- Liquidity Risk Management and Exposure
- Capital Adequacy
- Market Risk Management and Exposure
- Accounting Accuracy
- Internal Control Systems Design and Adequacy

- Audit Adequacy
- Information Technology and Information Security Risk Management and Exposure
- Anti-Money Laundering / Countering the Financing of Terrorism Risk and Compliance
- Operational Risk Management and Exposure
- Third Party Risk Management
- Permissibility (in consultation with Legal)
- Governance
- Framework for compliance with Applicable Laws and Regulations

Consumer Protection:

- Compliance with Applicable Consumer Protection Laws and Regulations, including Laws Related to Unfair and Deceptive Acts or Practices
- Potential for Consumer Harm or Customer Confusion
- Effectiveness of Compliance Management System
- Third Party Risk Management
- Potential Misrepresentations or False Advertising Regarding Deposit Insurance

If the Region's final assessment determines the risk management framework (e.g., risk assessment, due diligence) or compliance management system are not sufficient or significant risks are identified, the Region should determine what supervisory actions are appropriate in accordance with existing policies and procedures contained in the Risk Management Manual of Examination Policies and Consumer Compliance Examination Manual.

iv. Supervisory Feedback to the Institution

Once the review of safety and soundness and consumer protection considerations is complete, and the Region has consulted with the WO, the Region should provide feedback to the institution. The type of feedback provided will vary depending on various factors, including the type and complexity of activity, institution risk profile, and results of the review (such as level of concerns and findings). The format of the feedback will vary depending on whether a more formal examination activity is planned or in process that includes an assessment of the crypto-related activity.

If the activity is reviewed during, or results in the initiation of, a RMS/DCP visitation or examination, comprehensive feedback will generally be provided through the visitation or examination communication process. If the activity is reviewed outside of an examination activity, comprehensive supervisory feedback and any supervisory recommendations, as appropriate, should be communicated to the institution in writing on official FDIC letterhead. Comprehensive feedback shall include both safety and soundness and consumer protection considerations.

Supervisory feedback to the institution should specify whether additional actions or follow-up is necessary and establish a timeframe for the follow-up. If the feedback

includes supervisory recommendations, matters requiring board attention, or informal or formal enforcement actions, follow-up and closure should be performed consistent with outstanding instructions. If no additional action or follow-up is necessary, the supervisory feedback should specify to the institution that the FDIC's review is complete.

All proposed feedback to the institution or proposed supervisory actions regarding crypto-related activities, in any form, such as a letter, examination/visitation transmittal, or other official FDIC communication, must be reviewed by the designated WO RMS and DCP personnel (except as noted above related to the use of templates). The final supervisory feedback should be retained in [redacted].

v. Signature Authority

All letters to the institution (including, but not limited to, requests for additional information or out of scope letters) and all transmittal letters to the bank with supervisory feedback or recommendations must be signed by the Regional Director or by both RMS and DCP Deputy Regional Directors (underlying reports can continue to be signed under standard delegations).

d. Washington Office Collaboration

Due to the evolving risks and concerns that exist with crypto-assets and crypto-related activities, collaboration between the Regions and WO is designed to ensure the objectives of the FIL are supported by effectively sharing knowledge and resources. To ensure consistency in the review processes and feedback, the Case Manager and Review Examiner (or other designated DCP regional point of contact), or examination team (in the case of a visitation or examination) should collaborate with the WO throughout the review. This collaboration will be especially close when the activity involves: 1) a third party that is providing the same crypto-related activity to multiple banks across the country, 2) multiple banks collaborating to offer a crypto-related activity (such as through a network or consortium), or 3) a unique crypto-related activity that has not previously been identified and reviewed.

Collaboration includes:

- WO review of information in the tracking system.
- Regional RMS/DCP staff providing WO personnel with access to information submitted by the institution (to the extent not included in [redacted]).
- Regional RMS/DCP staff consulting with designated WO personnel to collaboratively review information submitted by the institution, develop follow-up requests, and recommend any supervisory plan changes, such as scheduling an accelerated examination or visitation.

4. <u>Effective Date</u>: The procedures in this RD Memo are effective immediately.

5. <u>Distribution</u>: This RD Memo should be distributed to all RMS and DCP personnel.

6. **Attachments**: [redacted]
   Request List: Facilitation of Customer Purchase and Sale of Crypto-Assets Through Institution with Third Party
   Request List: Crypto-Asset Collateralized Lending
   Acknowledgment and Out-of-Scope Letter

7. **References**: FIL-16-2022 Notification of Engaging in Crypto-Related Activities
   [redacted]

Request List: Facilitation of Customer Purchase and Sale of Crypto-Assets Through Institution with Third Party

Note: This information request list may be utilized for institutions that offer customers products and services to buy, sell, and hold crypto-asset in conjunction with a third party. Consider what information an institution provided in the initial notification and customize this template as appropriate to prevent duplicate information requests and to address any unique aspects of the activity. Placeholders highlighted in gray should be tailored to each bank's specific crypto activity prior to transmittal.

1. Contracts (including any draft contracts that bank is reviewing/considering).
2. Overview of the contracting process (e.g., who is/was involved in the review, analysis, and structuring).
3. Any contract analysis performed prior to execution.
4. Description of the transaction flows and related controls.
5. Detailed description of the settlement process for customer buy/sell transactions between the bank, [ ], and any other related parties.
6. The bank's independent permissibility analysis and determination with respect to the activity.
7. Bank's analysis of Securities and Exchange Commission Staff Accounting Bulletin 121 and its applicability.
8. Cost-benefit analysis for the activity.
9. Project plan for the activity.
10. Vendor management due diligence documentation and analysis related to both [, , or other third party name] and [ ], including audits, financials, insurance, complaints, compliance with U.S. AML and sanctions requirements, etc.
11. Description of what happens to customers' accounts or holdings [ ] if the bank does not continue or cancels offering the services provided by [, or other third party name], or if the third party cancels or fails to perform under the contract.
12. Description of any fees that will be charged to customers related to the activity, and how they will be calculated. Also, describe if and how fees are split among the bank and any third parties involved in the activity.
13. Description of any transaction limitations imposed by [ ] or the bank on the amount [ ] a customer may purchase or sell (e.g. daily, weekly, monthly).
14. Description of transaction monitoring processes in place to identify and report suspicious activity associated with customer transactions between the bank and [ ].
15. Description of the methodology that determines the price customer pays to [ ] for [ ]. This includes providing an explanation of how any market price is determined and how the spread, if any, is calculated.

16. Customer agreements, disclosures, sample account statement, sample transaction receipt, and other terms and conditions related to the activities provided by or through the bank and by third parties (draft or proposed).
17. Marketing materials, press releases, internal scripts, educational materials, and any other publicly-distributed information related to the activity (draft or proposed). This includes screen shots/screen recordings of any online banking or mobile application user interfaces (including hidden text that must be clicked) that will be made visible to customers by, or through, the bank in connection with activity. Also, a live demonstration of the user interface of the online banking or mobile application customer experience may be requested during the review of this activity.
18. Any other due diligence materials.
19. Describe how this crypto-asset activity fits into the bank's strategic plan and objectives of the board and actions that would be taken should the activity fail to achieve the objectives.
20. Implementation plan. Please include expected activity volumes, income projections used to determine whether the products are financially feasible, and any other analysis performed to support launching the products.
21. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activity.
22. Risk assessment(s) related to the activity.
23. Internal training materials related to the activity.
24. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution.
25. If not outlined in policies and procedures, framework of assigned responsibilities and qualifications for those involved in day-to-day administration of crypto-related activity, including internal controls responsibilities. Description of oversight responsibilities (e.g. management, staff, committees (including members, frequency of meetings), and collectively, their approval authority).
26. If program is Live/Beta Testing, provide transaction volumes that include: 1) number of active accounts using this service through bank, 2) total number and dollar volume of buy transactions completed (since implementation), and 3) total number and dollar volume of sell transactions completed (since implementation).

Request List: Crypto-Asset Collateralized Lending

Note: This information request list may be utilized for institutions that offer commercial loans collateralized by crypto-assets. Consider what information an institution provided in the initial notification and customize this list as appropriate to prevent duplicate information requests and to address any unique aspects of the activity. Placeholder highlighted in gray should be completed prior to transmittal to the institution.

1. Loan and security agreements.
2. Loan policy and customer eligibility criteria related to crypto-asset collateralized lending and associated underwriting standards/procedures.
3. Risk assessment (related to decision to enter into crypto lending).
4. Provide a description of bank's expertise in this type of lending, or how it will build expertise.
5. Describe how this crypto-asset activity fits into the bank's strategic plan and objectives of the board and actions that would be taken should the activity fail to achieve the objectives.
6. Please include expected volumes of activity, income projections used to determine whether the products are financially feasible, and any other analysis performed to support launching the products.
7. Documentation of analysis related to selection of which crypto assets to accept as collateral, loan pricing, collateral thresholds, concentration limits.
8. Board minutes reflecting approval, discussion, analysis, and any documentation provided to the board on the activity.
9. Loan committee minutes reflecting approval, discussion, analysis, and any documentation provided to the committee on the activity (including credit memo).
10. Borrower and guarantor financials and associated analyses.
11. Bank's analysis of Securities and Exchange Commission Staff Accounting Bulletin 121 and its applicability and any accompanying opinion of counsel.
12. Bank's legal analysis and determination with respect to permissibility of lending activity collateralized by crypto-assets, as well as legal analysis related to ownership of the crypto-assets serving as collateral, authority to pledge the crypto-assets serving as collateral, security interest perfection, and foreclosure on the crypto-asset collateral, and any accompanying opinion of counsel.
13. If collateral involved is rehypothecated collateral tendered by the borrower's clients, documentation of borrower's authority to rehypothecate (such as from the borrower's underlying financing arrangements) and analysis of the adequacy and enforceability of the borrower's documentation.
14. For any collateral custodians and entities that provide collateral maintenance functions
    a. Contracts or agreements
    b. Risk assessment and due diligence
    c. Analysis of bankruptcy implications performed by the bank
    d. Ongoing monitoring
15. Detailed description of the information technology arrangement or infrastructure utilized for collateral maintenance function, including all data flows, interfaces with bank's core systems, and new IT development and costs to implement/facilitate.

16. Detailed description of the collateral maintenance monitoring function.
17. Bank reporting on collateral maintenance monitoring.
18. Describe how crypto-asset lending activities will be monitored to identify and report suspicious activity.
19. Independent credit review documentation.
20. For each credit: origination balance; balance as of [enter date]; margin call history (when margin calls were made and met, and amounts); and for lines of credit, amount, date, and length paydowns/clean ups.
21. Capital risk weighting treatment of the credit.
22. Loan loss reserve associated with such loans.
23. Bank's conflict of interest/ethics/conduct policy.
24. Marketing materials, press releases, and any other publicly distributed information related to the activity (draft or proposed).
25. Any documents used to support internal training of staff or directors on the proposed activities.

Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
Street, City, State Zip

[Name] Regional Office
Phone (xxx) xxx-xxxx
Fax (xxx) xxx-xxxx

January 2, 2025

Board of Directors
ABC Bank
123 Main Avenue
City, State 12345

Subject: Notification of Engagement in Crypto-Related Activities

Dear Members of the Board:

The FDIC acknowledges the notification provided by [insert bank name]'s (the Bank) on [insert date notification was received], regarding the Bank's [engagement in or intent to engage in] [provide brief description of the type of activity(ies) included in the notification]. 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.

The notification states that [provide detailed description of the activity(ies) that are out of scope in order to ensure it is clear to the bank exactly what we understood about a given activity that led us to determine it was out of scope from the review and feedback process described in the FIL].

Upon review of the information provided by the Bank, we have determined that the activity(ies) described by the Bank in its notification fall outside the scope of the review and feedback process described in FIL-16-2022. However, if the scope of the activity changes or is other than as described, please notify us, as a change in facts may change the scope determination. Further review of these activities may occur as part of our normal supervisory process.

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 [Name] at [Number] or Review Examiner [Name] at [Number]. Written correspondence should be addressed to my attention at the [Name] Regional Office, and sent as a

PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: [Regional Mail Room Email].

Sincerely,

[Name]
Regional Director

cc: [Name of State Banking Agency]