DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

March 27, 2025

VIA ELECTRONIC MAIL

Josh Shear
300 N Stonestreet Ave
Rockville, MD 20850

Email: jshear@historyassociates.com

RE: Your FOIA Request to Treasury, Case Number 2024-FOIA-01526

Dear Mr. Shear:

This is the final response of the Department of the Treasury (Treasury) to the Freedom of Information Act (FOIA) request you filed with the Federal Deposit Insurance Corporation (FDIC) dated March 31, 2023. You requested:

"1. All documents and communications, both written and electronic, exchanged between members of the FDIC Board of Directors and/or FDIC staff members, including, but not limited to staff of the Division of Administration, Division of Complex Institution Supervision and Resolution, Division of Depositor and Consumer Protection, Division of Finance, Division of Information Technology, Division of Insurance and Research, Division of Resolutions and Receiverships, Division of Risk Management Supervision, the Legal Division, Office of Communications, Office of Legislative Affairs, Office of Risk Management and Internal Controls, and Office of Inspector General, and staff of the following federal and state agencies:

a. U.S. Department of the Treasury
b. Office of the Comptroller of the Currency
c. Securities and Exchange Commission
d. United States Federal Reserve System
e. National Economic Council
f. U.S. Department of Justice Office of the Attorney General
g. New York State Department of Financial Services
h. California Department of Financial Protection and Innovation

2. That refers, relates, or discusses the February 23, 2023, joint statement of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency, entitled "Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities," and available at the following link: https://www.fdic.gov/news/press-releases/2023/pr23010a.pdf,
3. And was sent between the publication of the joint statement on February 23, 2023, and the date you process this request."

In a memo dated September 9, 2024, the FDIC referred 24 pages of potentially responsive documents to Treasury for review, processing, and direct response to you. Treasury processed this request under the provisions of the FOIA, 5 U.S.C. § 552.

After carefully considering these records, Treasury is releasing 6 pages in full. Treasury is also withholding 18 pages in full. The withheld information is protected from disclosure under the FOIA pursuant to 5 U.S.C. § 552 (b)(5) and (b)(6).

FOIA Exemption 5 exempts from disclosure "inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency." This includes communications forming part of the deliberative process, attorney-client privilege, or attorney work product.

FOIA Exemption 6 exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

Treasury has considered the foreseeable harm standard when reviewing the records and applying these exemptions.

There are no fees assessed at this time since allowable charges fell below $25.

Since Treasury's response constitutes an adverse action, you have the right to appeal this determination within 90 days from the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. Your appeal must be in writing, signed by you or your representative, and should contain the rationale for your appeal. Please also cite the FOIA reference number noted above. Your appeal should be addressed to:

FOIA Appeal
FOIA and Transparency
Office of Privacy, Transparency, and Records
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

If you submit your appeal by mail, clearly mark the letter and the envelope with the words "Freedom of Information Act Appeal." Your appeal must be postmarked or electronically transmitted within 90 days from the date of this letter.

If you would like to discuss this response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact our FOIA Public Liaison for assistance via email at FOIAPL@treasury.gov, or via phone at (202) 622-8098. A FOIA Public Liaison is a supervisory official to whom FOIA requesters can raise questions or concerns about the agency's FOIA process. FOIA Public Liaisons can explain agency records, suggest agency offices that may have responsive records, provide an estimated date of completion, and discuss

how to reformulate and/or reduce the scope of requests in order to minimize fees and expedite processing time.

If the FOIA Public Liaison is unable to satisfactorily resolve your question or concern, the Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may contact the agency directly by email at OGIS@nara.gov, by phone at (877) 684-6448, by fax at (202) 741-5769 or by mail at the address below:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001

Please note that contacting any agency official (including the FOIA analyst, FOIA Requester Service Center, FOIA Public Liaison) and/or OGIS is not an alternative to filing an administrative appeal and does not stop the 90-day appeal clock.

You may reach me via telephone at 202-622-0930, extension 2; or via email at FOIA@treasury.gov. Please reference FOIA case number 2024-FOIA-01526 when contacting our office about this request.

Sincerely,

Shirley Brown
Senior FOIA Specialist
for Mark Bittner
Director for FOIA and Transparency
Office of Privacy, Transparency, and Records

Enclosures
Responsive document set in redacted format (24 pages)

Page 01 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

January 3, 2023

Joint Statement on Crypto-Asset Risks to Banking Organizations

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing the following statement on crypto-asset[1] risks to banking organizations.

The events of the past year have been marked by significant volatility and the exposure of vulnerabilities in the crypto-asset 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:

- Risk of fraud and scams among crypto-asset sector participants.
- Legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings.
- Inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties.
- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.
- Susceptibility of stablecoins to run risk, creating potential deposit outflows for banking organizations that hold stablecoin reserves.
- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements. These interconnections may also present concentration risks for banking organizations with exposures to the crypto-asset sector.
- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.
- Heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance.

It is important that risks related to the crypto-asset sector that cannot be mitigated or controlled do not migrate to the banking system. The agencies are supervising banking organizations that may be exposed to risks stemming from the crypto-asset sector and carefully reviewing any

[1] By "crypto-asset," the agencies refer generally to any digital asset implemented using cryptographic techniques.

proposals from banking organizations to engage in activities that involve crypto-assets. Through the agencies' case-by-case approaches to date, the agencies continue to build knowledge, expertise, and understanding of the risks crypto-assets may pose to banking organizations, their customers, and the broader U.S. financial system. Given the significant risks highlighted by recent failures of several large crypto-asset companies, the agencies continue to take a careful and cautious approach related to current or proposed crypto-asset-related activities and exposures at each banking organization.

Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation. The agencies are continuing to assess whether or how current and proposed crypto-asset-related activities by banking organizations can be conducted in a manner that adequately addresses safety and soundness, consumer protection, legal permissibility, and compliance with applicable laws and regulations, including anti-money laundering and illicit finance statutes and rules. Based on the agencies' current understanding and experience to date, the agencies believe that issuing or holding as principal crypto-assets that are issued, stored, or transferred on an open, public, and/or decentralized network, or similar system is highly likely to be inconsistent with safe and sound banking practices. Further, the agencies have significant safety and soundness concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector.

The agencies will continue to closely monitor crypto-asset-related exposures of banking organizations. As warranted, the agencies will issue additional statements related to engagement by banking organizations in crypto-asset-related activities. The agencies also will continue to engage and collaborate with other relevant authorities, as appropriate, on issues arising from activities involving crypto-assets.

Each agency has developed processes[2] whereby banking organizations engage in robust supervisory discussions regarding proposed and existing crypto-asset-related activities.[3] Banking organizations should ensure that crypto-asset-related activities can be performed in a safe and sound manner, are legally permissible, and comply with applicable laws and regulations, including those designed to protect consumers (such as fair lending laws and prohibitions against unfair, deceptive, or abusive acts or practices). Banking organizations should ensure appropriate

[2] *See* OCC Interpretive Letter 1179 "Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank," (November 18, 2021); Federal Reserve SR 22-6 / CA 22-6: "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations," (August 16, 2022); and FDIC FIL-16-2022 "Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities," (April 7, 2022).

[3] Entities seeking to become regulated banking organizations will also be expected to adopt and demonstrate appropriate risk management processes and controls to mitigate risks associated with planned activities, which would include any crypto-asset-related activities, before receiving a charter or otherwise being authorized to commence business. The entities should discuss all planned activities with the appropriate regulator prior to filing an application.

risk management, including board oversight, policies, procedures, risk assessments, controls, gates and guardrails, and monitoring, to effectively identify and manage risks.[4]

[4] *See* Interagency Guidelines Establishing Standards for Safety and Soundness 12 CFR 30, Appendix A (OCC); 12 CFR 208, Appendix D-1 (Federal Reserve) and 12 CFR 364, Appendix A (FDIC). *See also* OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 12 CFR 30, Appendix D (OCC).

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

February 23, 2023

Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing this statement on the liquidity risks presented by certain sources of funding from crypto-asset[1]-related entities, and some effective practices to manage such risks.

The statement reminds banking organizations to apply existing risk management principles; it does not create new risk management principles.[2] Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

Liquidity Risks Related to Certain Sources of Funding from Crypto-Asset-Related Entities

This statement highlights key liquidity risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of.[3] In particular, certain sources of funding from crypto-asset-related entities may pose heightened liquidity risks to banking organizations due to the unpredictability of the scale and timing of deposit inflows and outflows, including, for example:

- **Deposits placed by a crypto-asset-related entity that are for the benefit of the crypto-asset-related entity's customers (end customers).** The stability of such deposits may be driven by the behavior of the end customer or crypto-asset sector dynamics, and not solely by the crypto-asset-related entity itself, which is the banking organization's direct counterparty. The stability of the deposits may be influenced by, for example, periods of stress, market volatility, and related vulnerabilities in the crypto-asset sector, which may or may not be specific to the crypto-asset-related entity. Such deposits can be susceptible to large and rapid inflows as well as outflows, when end customers react to

[1] A crypto-asset generally refers to any digital asset implemented using cryptographic techniques.

[2] *See* Interagency Policy Statement on Funding and Liquidity Risk Management, Federal Reserve SR 10-6 (March 17, 2010), FDIC FIL-13-2010 (April 10, 2010), and OCC Bulletin 2010-13 (March 22, 2010). For bank holding companies and foreign banking organizations with $100 billion or more in total consolidated assets, *see* 12 CFR 252.34 and 12 CFR 252.156, respectively. For national banks and Federal savings associations, *see also* OCC Interpretive Letter 1172, "OCC Chief Counsel's Interpretation on National Banks and Federal Savings Association Authority to Hold Stablecoin Reserves" (September 21, 2020) and OCC Interpretive Letter 1179, "Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank," (November 18, 2021).

[3] *See* Joint Statement on Crypto-Asset Risks to Banking Organizations (January 3, 2023).

crypto-asset-sector-related market events, media reports, and uncertainty. This uncertainty and resulting deposit volatility can be exacerbated by end customer confusion related to inaccurate or misleading representations of deposit insurance by a crypto-asset-related entity.[4]

- **Deposits that constitute stablecoin-related reserves.** The stability of such deposits may be linked to demand for stablecoins, the confidence of stablecoin holders in the stablecoin arrangement, and the stablecoin issuer's reserve management practices. Such deposits can be susceptible to large and rapid outflows stemming from, for example, unanticipated stablecoin redemptions or dislocations in crypto-asset markets.

More broadly, when a banking organization's deposit funding base is concentrated in crypto-asset-related entities that are highly interconnected or share similar risk profiles, deposit fluctuations may also be correlated, and liquidity risk therefore may be further heightened.

Effective Risk Management Practices

In light of these heightened risks, it is important for banking organizations that use certain sources of funding from crypto-asset-related entities, such as those described above, to actively monitor the liquidity risks inherent in such funding sources and establish and maintain effective risk management and controls commensurate with the level of liquidity risks from such funding sources. Effective practices for these banking organizations could include, for example:

- Understanding the direct and indirect drivers of potential behavior of deposits from crypto-asset-related entities and the extent to which those deposits are susceptible to unpredictable volatility.
- Assessing potential concentration or interconnectedness across deposits from crypto-asset-related entities and the associated liquidity risks.
- Incorporating the liquidity risks or funding volatility associated with crypto-asset-related deposits into contingency funding planning, including liquidity stress testing and, as appropriate, other asset-liability governance and risk management processes.[5]
- Performing robust due diligence and ongoing monitoring of crypto-asset-related entities that establish deposit accounts, including assessing the representations made by those crypto-asset-related entities to their end customers about such deposit accounts that, if inaccurate, could lead to rapid outflows of such deposits.[6]

In addition, banking organizations are required to comply with applicable laws and regulations. For insured depository institutions this includes, but is not limited to, compliance with brokered

---

[4] *See* Federal Reserve and FDIC, "Joint Letter Regarding Potential Violations of Section 18(a)(4) of the Federal Deposit Insurance Act," (July 28, 2022).

[5] *See* "Interagency Policy Statement on Funding and Liquidity Risk Management," 75 Fed. Reg. 13656 (March 22, 2010).

[6] *See* FDIC FIL-35-2022, "Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies," (July 29, 2022).

deposits rules,[7] as applicable, and Consolidated Reports of Condition and Income (also known as the Call Report) filing requirements.[8]

[7] *See* 12 CFR 337.6.

[8] *See* 12 USC 324 (Federal Reserve); 12 USC 1817(a) and 12 CFR 304.3 (FDIC); and 12 USC 161 and 1464(v) (OCC).

Page 20 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24 of 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act