

**OPERATION CHOKE POINT 2.0:
THE BIDEN ADMINISTRATION'S EFFORTS
TO PUT CRYPTO IN THE CROSSHAIRS**

HEARING
BEFORE THE
**SUBCOMMITTEE ON OVERSIGHT AND
INVESTIGATIONS**
OF THE
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

FEBRUARY 6, 2025

Serial No. 119–2

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

59–598 PDF

WASHINGTON : 2025

HOUSE COMMITTEE ON FINANCIAL SERVICES

FRENCH HILL, Arkansas, *Chairman*

BILL HUIZENGA, Michigan, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	SYLVIA R. GARCIA, Texas, <i>Vice Ranking Member</i>
PETE SESSIONS, Texas	NYDIA M. VELÁZQUEZ, New York
ANN WAGNER, Missouri	BRAD SHERMAN, California
ANDY BARR, Kentucky	GREGORY W. MEEKS, New York
ROGER WILLIAMS, Texas	DAVID SCOTT, Georgia
TOM EMMER, Minnesota	STEPHEN F. LYNCH, Massachusetts
BARRY LOUDERMILK, Georgia	AL GREEN, Texas
WARREN DAVIDSON, Ohio	EMANUEL CLEAVER, Missouri
JOHN W. ROSE, Tennessee	JAMES A. HIMES, Connecticut
BRYAN STEIL, Wisconsin	BILL FOSTER, Illinois
WILLIAM R. TIMMONS, IV, South Carolina	JOYCE BEATTY, Ohio
MARLIN STUTZMAN, Indiana	JUAN VARGAS, California
RALPH NORMAN, South Carolina	JOSH GOTTHEIMER, New Jersey
DANIEL MEUSER, Pennsylvania	VICENTE GONZALEZ, Texas
YOUNG KIM, California	SEAN CASTEN, Illinois
BYRON DONALDS, Florida	AYANNA PRESSLEY, Massachusetts
ANDREW R. GARBARINO, New York	RASHIDA TLAIB, Michigan
SCOTT FITZGERALD, Wisconsin	RITCHIE TORRES, New York
MIKE FLOOD, Nebraska	NIKEMA WILLIAMS, Georgia
MICHAEL LAWLER, New York	BRITTANY PETTERSEN, Colorado
MONICA DE LA CRUZ, Texas	CLEO FIELDS, Louisiana
ANDREW OGLES, Tennessee	JANELLE BYNUM, Oregon
ZACHARY NUNN, Iowa	SAM LICCARDO, California
LISA McCLAIN, Michigan	
MARIA SALAZAR, Florida	
TROY DOWNING, Montana	
MIKE HARIDOPOLOS, Florida	
TIM MOORE, North Carolina	

Ben Johnson, *Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

DANIEL MEUSER, Pennsylvania, *Chairman*

TIM MOORE, North Carolina, <i>Vice Chairman</i>	AL GREEN, Texas, <i>Ranking Member</i>
ANN WAGNER, Missouri	RASHIDA TLAIB, Michigan
BARRY LOUDERMILK, Georgia	NIKEMA WILLIAMS, Georgia
ANDREW GARBARINO, New York	CLEO FIELDS, Louisiana
ANDY OGLES, Tennessee	SAM LICCARDO, California
MIKE HARIDOPOLOS, Florida	

C O N T E N T S

Thursday, February 6, 2025

OPENING STATMENTS

	Page
Hon. Daniel Meuser, Chairman of the Subcommittee on Oversight and Investigations, a U.S. Representative from Pennsylvania	2
Hon. Al Green, Ranking Member of the Subcommittee on Oversight and Investigations, a U.S. Representative from Texas	3

STATEMENTS

Hon. French Hill, Chairman of the Committee on Financial Services, a U.S. Representative from Arkansas	4
--	---

WITNESSES

Mr. Austin Campbell, Acting CEO of Worldwide Stablecoin Payment Network (WSPN) U.S.A., Managing Partner and Founder of Zero Knowledge Consulting, Adjunct Professor, Stern School of Business, New York University ..	5
Prepared Statement	7
Mr. Paul Grewal, Chief Legal Officer, Coinbase Global, Inc.	25
Prepared Statement	27
Mr. Fred Thiel, Chairman of the Board of Directors and Chief Executive Officer, Marathon Digital Holdings (MARA)	225
Prepared Statement	227
Ms. Shayna Olesiuk, Director of Banking Policy, Better Markets	231
Prepared Statement	233

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

Hon. Daniel Meuser:	
The U.S. Department of Treasury	278
Hon. Maxine Waters:	
Public Citizen	279
The United States Cannabis Roundtable	283
Defense Credit Union Council (DCUC)	285

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Representative Maxine Waters	
Mr. Paul Grewal	287
Mr. Fred Thiel	288
Ms. Shayna Olesiuk	289

OPERATION CHOKE POINT 2.0: THE BIDEN ADMINISTRATION'S EFFORTS TO PUT CRYPTO IN THE CROSSHAIRS

Thursday, February 6, 2025

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:03 p.m., in room 2128, Rayburn House Office Building, Hon. Dan Meuser [chairman of the subcommittee] presiding.

Members Present: Representatives Meuser, Wagner, Loudermilk, Garbarino, Haridopolos, Moore, Waters, Green, Tlaib, Williams of Georgia, Fields, and Liccardo.

Also present: Representatives Hill, Davidson, Steil, and Downing.

Chairman MEUSER. Ladies and gentlemen, the Subcommittee on Oversight and Investigations will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time.

This hearing is entitled, "Operation Choke Point 2.0: The Biden Administration's Efforts to Put Crypto in the Crosshairs."

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record.

As a point of personal privilege, I want to say, this is our first hearing of Oversight and Investigations for the Financial Services Committee for the 119th Congress, so I appreciate very much everyone being here, and we look forward to a very productive, civil and worthwhile time together. I am pleased that we have our full committee chairman, Chairman Hill, with us.

Now, on another point of personal privilege, I would like to yield to our Ranking Member, Representative Al Green.

Mr. GREEN. Thank you, Mr. Chairman. I am honored to congratulate you on your new position, your new station in life. I do look forward to working with you. I welcome all of the members to the committee and would indicate that I appreciate your kindness and generosity in agreeing to allow me to have next-to-the-last opportunity to speak at committee hearings. Again, I am grateful.

Chairman MEUSER. Very good. Thank you.

I now recognize myself for 4 minutes to give an opening statement.

**OPENING STATEMENT OF HON. DANIEL MEUSER, CHAIRMAN
OF THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGA-
TIONS OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S.
REPRESENTATIVE FROM PENNSYLVANIA**

Chairman MEUSER. Today's hearing is entitled, "Operation Choke Point 2.0: The Biden Administration's Effort to Put Crypto in the Crosshairs." I would like to thank the witnesses very much for appearing before the committee today to share their experience, their great experience and expertise on this issue.

The Biden Administration's Operation Choke Point 2.0 was carried out by the prudential regulators to target and, in fact, debank the digital asset ecosystem. The Federal Deposit Insurance Corporation (FDIC) used offline conversations and threats of formal supervisory actions to pressure banks to deny service to digital asset firms, their employees, and even their customers. This is a serious abuse of regulatory power. Unfortunately, you would be wrong to assume this is the first attempt to debank an entire industry.

Beginning in 2013, Obama's Department of Justice enlisted bank regulators in the first iteration of Operation Choke Point. President Obama's Operation Choke Point targeted gun manufacturers, payday loan companies, our energy industry, and other businesses and legal industries that were disfavored by the Obama Administration. Their plan was straightforward, use the prudential regulators' authority to threaten supervisory action against banks who chose to provide services to these industries. After that, the bank has an ultimatum: continue to bank these customers under the looming threat of scrutiny or comply with the regulators' demands and remove that line of business from their books.

The Biden Administration broke out the same playbook. This time, their target was the digital asset ecosystem. Biden regulators resorted to vague, interpretive, regulatory letters threatening banks with negative examination scores and fines if they continue their partnership with digital asset companies. This is a serious overreach, one that only—not only undermines innovation, but directly harms consumers by restricting their access to new and beneficial financial products.

Acting FDIC, Chairman Travis Hill, just yesterday exposed Biden's Choke Point activities that debank crypto firms across the country. He said, "Requests from banks were almost universally met with resistance both individually and collectively." These and other actions sent the message to banks that it would be extraordinarily difficult, if not possible, to move forward. As a result, the vast majority of banks simply stopped trying to do business with crypto companies.

However, the FDIC promised to correct course moving forward, and I will continue to conduct oversight on their progress—we will continue to conduct oversight on their progress and determine legislative solutions—very much solutions, to emphasize—to make sure this does not happen again.

Access to capital and banking services are critical to the success of American businesses, and that is why I am looking forward to hearing from our witnesses today about how the regulators have been carrying this out, and to discuss solutions to make sure it

stops. The free market thrives when innovation is allowed to flourish. Regulators have a duty to protect our financial system, but not at the expense of legitimate businesses like energy and crypto companies.

I yield back.

The chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, Mr. Green, for 4 minutes for his opening statement.

OPENING STATEMENT OF HON. AL GREEN, RANKING MEMBER OF THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM TEXAS

Mr. GREEN. Thank you, Mr. Chairman.

Yes, the title of this hearing is, “Operation Choke Point 2.0: The Biden Administration’s Efforts to Put Crypto in the Crosshairs.” However, a better title for this hearing is how President Trump’s self-dealing deregulation will put well-intentioned investors at risk. The name, “Operation 2.0” refers to a fake program never initiated by the Biden Administration to restrict the cryptocurrency industry’s access to the banking system. The Biden Administration did not prohibit banks from dealing with cryptocurrency companies.

In January 2023, Federal financial regulators issued a joint statement warning banks about cryptocurrency asset risk, including, but not limited to, the risk of fraud and scams among crypto asset firms, the risk of inaccurate or misleading representations and disclosures by crypto asset companies, and many other risks.

In March 2023, Silvergate Bank and Signature Bank, two key crypto firms—pardon me, two key firms in the cryptocurrency banking industry failed in part due to their involvement with the digital asset sector. For example, between 2014 and 2021, the share of Silvergate’s crypto firm deposits increased from 1 percent of total deposits to a high of more than 98 percent.

The failure of these banks demonstrated that the concerns financial regulators had regarding bank exposure to cryptocurrency risk were well-founded. Regulators asking banks to consider the risk associated with the cryptocurrency industry does not amount to debanking, as my Republican friends are indicating. Regulators simply urged banks to exercise caution when dealing with this emerging and potentially risky industry.

Unfortunately, this hearing aid the Trump deregulatory pro-crypto agenda. As just days before President Trump’s Inauguration, he issued what I call a Money Trump Meme Coin that was heavily promoted on social media. Investors who may see this coin as a way to get rich quick may be overpaying for something of dubious value and could be left holding the bag after a sell-off.

Notably, the Money Trump Coin’s terms and conditions restrict buyers from bringing class-action lawsuits, even if they are swindled. Beyond the lack of investor protections and transparency, issuance of the Money Trump Coin also creates an avenue to circumvent national security and anti-corruption laws allowing any interested party, including adversaries and allies, to anonymously transfer money to the President and his family.

I yield back the balance of my time.

Chairman MEUSER. The gentleman yields.

The chair now recognizes the Chairman of the full committee, Mr. Hill, for 1 minute.

STATEMENT OF HON. FRENCH HILL, CHAIRMAN OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM ARKANSAS

Mr. HILL. I thank the chairman. Congratulations, Chairman Meuser, for your first hearing on this important topic.

I want to thank our witnesses for being with us today and sharing your views.

Access to banking services is critical to building a successful business and to growing our thriving economy. Consider what happens when a bank refuses to provide services to your company at the direction of a bank regulator. That is exactly what was happening under the Biden-Harris' policy of Operation Choke Point 2.0, which nearly severed the digital asset ecosystem from financial institutions. Our regulators' highest priority should be promoting safety and soundness—true—at all of our financial institutions but not picking winners and losers.

We saw this not only in our bank supervision, but also at the Securities Exchange Commission (SEC) where one of our witnesses today, Coinbase, an American company, registered as a public company with the SEC was treated poorly, and Future Exchange Trading Ltd. (FTX), a criminal organization, was not even investigated. Yield back.

Chairman MEUSER. The gentleman yields.

We will now go to our witnesses, and I will have the honor of introducing each.

First, we have—our first witness, Mr. Austin Campbell. Mr. Campbell is the Acting CEO of Worldwide Stablecoin Payment Network (WSPN) U.S.A., Managing Partner and Founder of Zero Knowledge Consulting, and Adjunct Professor at New York University Stern School of Business. Previously, Austin has held multiple roles in the financial world, including running trading desks at J.P. Morgan and Citi (Citibank) for over a decade, running the stablecoin platform at Paxos, and being a Portfolio Manager and Structure at Stone Ridge and New York Digital Investment Group, LLC (NYDIG). Welcome.

Our next witness is Mr. Paul Grewal. Paul Grewal is the Chief Legal Officer of Coinbase Global, Inc., where he is responsible for Coinbase's legal compliance, global intelligence, and government relations groups. Before joining Coinbase, Paul was Vice President and Deputy General Counsel at Facebook and served as U.S. Magistrate Judge for the U.S. District Court for the Northern District of California. Thank you very much for being here.

Next is Mr. Fred Thiel, the Chairman of the Board of Directors and Chief Executive Officer of Marathon Digital Holdings (MARA). He has over 35 years of extensive experience in the technology sector. He is an acclaimed innovator and expert, having led organizations across diverse fields, including digital assets, artificial intelligence (AI), semiconductors, and enterprise software. I appreciate you being here.

Our last witness is Ms. Shayna Olesiuk. She is the Director of Banking Policy at Better Markets. She previously was the Deputy Director of the Division of Insurance and Research at the FDIC and has more than 25 years of public sector nonprofit experience in banking, finance, and economics.

Again, we thank you all for taking your time to be here. Each of you will be recognized for 5 minutes to give an oral opening presentation of your testimony. Without objection, your written statements will be made part of the record.

Mr. Campbell, you are now recognized for 5 minutes for your remarks.

STATEMENT OF AUSTIN CAMPBELL, ACTING CEO OF WSPN U.S.A., MANAGING PARTNER AND FOUNDER OF ZERO KNOWLEDGE CONSULTING, AND ADJUNCT PROFESSOR, STERN SCHOOL OF BUSINESS, NEW YORK UNIVERSITY

Mr. CAMPBELL. Thank you, Chairman Meuser and thank you to the entire committee for the opportunity to testify today, and all the staffers working behind them to make this happen.

Chairman MEUSER. Mr. Campbell—

Mr. CAMPBELL. Yes.

Chairman MEUSER [continuing]. is your mic on?

Mr. CAMPBELL. My mic appears to be on.

Chairman MEUSER. All right.

Mr. CAMPBELL. Is this better?

Chairman MEUSER. That is better. Thank you.

Mr. CAMPBELL. All right. Excellent. Thank you, Chairman Meuser, appreciate the opportunity to testify today, and all of the members and staff working on this hearing.

Today, we are here to talk about Operation Choke Point 2.0, which everybody will note means there was an Operation Choke Point 1.0 prior to this Congress that also had to be addressed. Before we get to the specifics of the crypto industry, I would say this indicates we have a governance issue with banking regulation writ large. The fact that supervision is often confidential, hidden, and nobody knows exactly what happened itself is a problem that leads to abuse. I would suggest to the committee that without addressing this there will be hearings on Operation Choke Point 3.0 and 4.0 and 5.0 onward to infinity.

What happened with 2.0? It was an attempt to debank the crypto industry in America, and by debank, I want to be specific and say the denial of banking services that are considered basic and fundamental to operating a business. This is not, you do not get approved for a mortgage. This is not, you do not get a loan on favorable terms. This is, I cannot get a checking account to make payroll, to pay rent, to pay utilities, to pay taxes. It is that specific area where there were severe problems for crypto companies from 2022 to present within the U.S. financial system.

There was a document dropped from the FDIC yesterday that highlights some of these problems, but within it, you will see specific mentions of crypto companies being denied accounts because regulators would not approve new banking activity. You will see specific clients being limited or eliminated by banks because regulators told them they were not allowed to bank them, and you will

see a concerted campaign to characterize all forms of activity touching the crypto space as illicit or extremely incompatible with safety and soundness guidelines.

How does this work? The FDIC has a rubric called, Capital adequacy, Asset quality, Management earnings, Liquidity, and Sensitivity (CAMELS), and I am sorry, it does not refer to the animal. That is an acronym that they use to actually think about bank risk, and it covers things like capital, assets, liquidity, objective and verifiable concerns. The dangerous one is the letter in the middle, the hump in CAMELS, the M, and this is management. Management serves as a subjective measure of a banking regulator's belief of the competence or behavior of the management of a bank. Importantly, whatever your CAMELS rating is, it is the ceiling on your total rating as a bank.

If I have a bank that does nothing but take money for checking accounts and buys Treasury Bills (T-bills) which would be the safest bank in the entire ecosystem in the United States of America, but a banking regulator decides for subjective reasons that management is poor and downgrades them. That bank could be put out of business purely on the subject of judgment of a regulator in private, as all of that will remain confidential.

This is a vehicle for abuse, and it is also an area where the safety and soundness concerns, which on a stand-alone basis are legitimate, become warped, and they can be used as a tool to discriminate against industries, against individuals on any basis people want because it is not discoverable.

In my written testimony, I go into this in greater detail, but I believe there are important reforms this committee should consider with regard to how this behavior happens in the banking space. A simple one is that all banking guidance should be written. Do not allow verbal guidance, do not allow hearsay and subjective statements, write it down. Second, that guidance should be made public on some trailing basis. Once you have a paper trail of what the regulators are doing, we will be having many less of these hearings. We will know exactly what has happened. When banks refuse people's services, they should have to tell them why, and those statements should be written, complete, and transparent.

Last, they should abolish management and reputational risk as components of the rating of banks. Those are subjective, ripe for abuse, and can be used for really any ends that a banking regulator would like to wedge into an otherwise relatively objective framework.

Finally, I am a professor. I would not let any of my students grade their own homework. You should not be letting the banking regulators grade their own work here either. Agency decisions should be subject to outside oversight. Do not let a banking regulator like the FDIC be judge, jury, and executioner in private.

Thank you, Chairman.

[The prepared statement of Mr. Campbell follows:]

Testimony of J. Austin Campbell

CEO, WSPN USA
Managing Partner, Zero Knowledge Consulting
Adjunct Professor, NYU Stern School of Business

INTRODUCTION

First of all, let me thank Chairman Hill, Subcommittee Chair Meuser, Ranking Member Waters, and Subcommittee Ranking Member Green for the opportunity to testify today. I would also like to take a moment to thank all of the staff who have worked on this hearing. My job is the easy one: I get to write and speak, but there are dozens of hardworking folks behind the scenes who make everything happen on behalf of America. Thank you.

Secondly, I want to say it is an honor to be able to testify on this topic, and I believe it is one that is of utmost importance for all Americans. I will lay this out in my testimony below, but if you read nothing else and stop at this line, let me just say this: fair, transparent, and open access to financial services is something all law-abiding Americans deserve and is essential to preserving our system and way of life.

Should you listen to me¹? My CV is included with this testimony, so here is the summary version: I've spent more than a decade on wall street running trading desks and managing risks directly related to bank capital and market structure for more than a decade. I've built regulated financial products in crypto (they exist!) that served consumers well and did not lose people money. I founded a blockchain consulting firm. I'm a senior advisor to one of the key government subcontractors, Inca Digital, helping to fight financial crime in the crypto and traditional space. They work with entities like the Defense Advance Research Projects Agency, the Federal Reserve, and the CFTC (among others), and are busy suing crypto scammers to get money back for victims. In short, I care about our system working properly, consumers being protected, criminals being prosecuted, and people being treated fairly.

OVERVIEW

We are here today to discuss Operation Chokepoint 2.0, in which the US banking regulators managed to almost completely deprive an industry of access to basic banking services from the 2022-2024 period.

¹ This is the point where my wife would likely warn you about my terrible sense of humor if she were writing this

I will start by stating that the fact that we are having this discussion again, after Congress was already forced to confront Operation Chokepoint 1.0, is the most significant problem. Repeat occurrences of major issues are a sign of a deeper governance failure. This subcommittee faces the unenviable task of unpacking that problem, and I call it unenviable because much of the evidence the committee would need for a truly clear determination of exactly what happened is being obfuscated behind a cloak of confidentiality and transparency which could easily be disguising lawless actions or illegal discrimination. But how would we know, when it's all confidential? This is why we are here. Again.

Today it is the crypto industry facing a banking chokepoint, and in the past it has been payday lenders, firearm manufacturers, telemarketers, and other often disfavored industries. Some of that disfavor is earned! There are certainly some bad actors that have been in crypto (FTX & TerraForm Labs, for example) I could point to. However, that does not justify a regulatory response where entire industries, much of which did not engage in bad or illegal conduct, suffer collective punishment for the sins of the few and, to add insult to financial injury, this punishment is decided behind closed doors, obfuscated, denied, covered up, and leaves the victims deprived of any due process or recourse.

Speaking bluntly, unless you trust all future presidents of both political parties, no matter how extreme they are on the left or the right, to treat even their most hated foes with the utmost integrity, this is a problem.

Later, I unpack what I think happened with Chokepoint 2.0, the pernicious effects on an entire industry, and the many undeserving victims of this behavior who were lumped in with some of the bad actors. Here, however, I want to put the most important point first: it is essential Congress reforms banking supervisory practices to ensure that, years down the road, we are not holding hearings on Operation Chokepoint 3.0, 4.0, 5.0, 6.0, and onward to infinity². It is also obvious that the crypto space was denied adequate banking services, and the confidential nature of these discussions are making it impossible to determine precisely how or why that happened, which again is itself the problem.

To that end, the most important reform possible is the elimination of both confidential and verbal guidance by banking regulators. All supervisory guidance should be written, and verbal guidance alone without being put in writing should be cause for immediate termination and personal liability for banking regulators. In addition to this, all guidance should be made public, with no redactions other than for personally identifying information of bank clients³, on a 12 month trailing basis.

² Countable infinity, for you other math majors out there, in this case

³ Yes, this means both bank employees and regulators should be named - if you don't like that, maybe levered lending with other people's money and a government-granted charter is not for you?

There is no problem so severe that becoming public knowledge after a year of time to remediate it should be fatal for a bank, or if a problem is that severe, the bank should simply be shut down.

Additionally, when a bank fires a customer, they should have to tell them why, in writing. The only requirements around this notification should be that it is truthful and provides a clear explanation of why the relationship was terminated. Customer is not profitable due to low balances? So be it. The bank doesn't like the color of their shirt? Weird, but acceptable. The bank is closing the account because the regulator pressured them? Yes, this should also be disclosed. These two reforms alone would end the ability to run something like Operation Chokepoint 1.0 or 2.0, because all the dirty laundry would be aired out in public and a fact pattern of why customers were losing accounts would be documented in writing.

The greatest imperative before this subcommittee and Congress is to eliminate the secrecy behind debanking, which acts as potential cover for impermissible and illegal actions, and to solve this problem. We must ensure fairness for all Americans, especially the poor and politically disfavored who have the least power to fight back, by bringing these actions into the light.

WHAT IS DEBANKING

Many of us have been fired from jobs, but how many people have been fired from a bank? The experience may not be what you think.

In the good version, the bank gives you a warning and adequate advance notice to have your affairs in order: something like 60 or 90 days to move your accounts, and a request for instructions as to where to send all the money.

In the bad version, you get a letter in the mail two days after you figured out something was wrong because your debit card suddenly stopped working and all your automated payments start bouncing, and helpfully when you call your bank they tell you to reference the letter⁴ and refuse to otherwise talk with you. What does that letter say? It tells you that you are fired as a customer, forever, to never speak to them again, and included is a paper check for your remaining balance, which means you have to find a new bank that will open an account for you, deposit the check, and then finally you have access to your own money again.

This is assuming you can find another bank.

There are some important details about this process:

⁴ This is the one you won't receive for another two days

The first is that there is no requirement for you to be given an explanation by the bank. They can just close your account, tell you that they will not explain why, and that it is final. There is also no meaningful appeal⁵. It just happens.

The second is that they may not limit it to you. They may also debank your relatives (spouse, children, parents, etc.) as well as you, so that if you didn't already have multiple banking relationships at multiple entities, the web of disruption now spreads to your entire family. The same is true of corporations - they could wipe out an entire tree of corporate entities in a single fell swoop, and this can cripple or bankrupt enterprises.

You will notice I have focused here on closing of accounts and denial of basic services. This is because debanking is an often confused topic, so I want to be clear about what we are discussing: I would describe debanking as what happens when you are denied the core, low-risk, extremely necessary services of regular banking (e.g. checking accounts) and payments (e.g. debit cards, ACH).

Being denied a mortgage is not necessarily debanking. Being denied a credit card is not necessarily debanking. Being denied corporate financing is not necessarily debanking. Debanking is when the core services a business needs to operate (access to deposits, payments, and in some cases, custody services for money) are denied.

Why define it this way? As a former trader and bank risk person myself, there are very legitimate business reasons to decline to lend or extend credit to many institutions that have nothing to do with impermissible bias⁶, speaking as someone who has said "no" to a lot of trades, possibly in significantly less polite language that I won't repeat here.

However, there is almost no economic reason⁷ to deny someone a checking account except for:

1. You think their balances will be too small to justify the costs of servicing them
2. You don't want their kind of business at all because you see significant AML / CTF style risks
3. Your regulator has threatened to make your life extremely difficult for taking them on

Fundamentally, taking deposits is not risky! The lending part? That tends to cause a lot of problems when you try to get fancy. However, the act of taking deposits, paying depositors the

⁵ Unless you are super politically connected or able to put them on blast publicly in ways that would be worse for them than keeping you

⁶ There may be a bias in overestimating volatility or default risk due to unfamiliarity in new asset classes, but that is more routine risk professional conservatism

⁷ There are niche complaints about things like chargebacks, but those are not unique to crypto (imagine Amazon having a huge fulfillment issue!) and if that is the real concern, we should be reforming ACH, not denying people accounts

national average checking account interest rate of 0.07%⁸, and then putting that money into treasury bills earning you well over 4%⁹ if you buy them on the secondary market should not be risky¹⁰. And yet, given that basic deposit account services of this type are essentially free money for banks from this perspective, people are still getting debanked all the time! What is happening?

OPERATION CHOKEPOINT 2.0:

A MOST UNWELCOME SEQUEL

That brings me to the topic of this hearing: from 2022 until the present, crypto companies have faced severe problems getting bank accounts in America.

First, I want to start by stating that I am not championing the case of entities like FTX, Celsius, or the like. These were entities run by criminals, doing criminal things, and it is not unfair or unreasonable for them to be debanked, along with employees being thrown in jail and entities being shut down. Good riddance. Had the actions of banking regulators stopped there, I would be quite complimentary of them in this hearing¹¹.

However, debanking did not stop there. Completely unrelated companies lost their operating accounts, such as those in the bitcoin mining space, such as blockchain foundations who had banked at Signature or Silicon Valley Bank and, upon their collapse, were all but unable to establish new accounts. Companies that were creating digital art on blockchains? Debanked or refused accounts. Companies that merely create software for things like validators, wallets, or blockchain explorers? Same story. Even my own consulting company, which does no actual hands-on work in crypto and just advises people, was denied a bank account by at least one bank because of "crypto exposure". There are multiple startups who simply couldn't get accounts at all and now exist offshore or had converted into solely on-chain entities with remote employees paying for things with stablecoins.

This is where I want to take a moment to stress that we are not talking about accounts where crypto companies somehow hold crypto on the balance sheet of banks. Neither are we talking about accounts that are being used for leveraged trading, such as hedge fund prime brokerage style arrangements. Again, we are talking about accounts for making payroll, for paying rent, for

⁸ <https://www.fdic.gov/national-rates-and-rate-caps>

⁹

https://home.treasury.gov/resource-center/data-chart-center/interest-rates/TextView?type=daily_treasury_bill_rates&field_tdr_date_value=2025

¹⁰ Seriously, if you can't manage this, you shouldn't be a bank or handling other people's money at all!

¹¹ We wouldn't be having this hearing at all, in fact

safely holding customer money, or for receiving money after raising a round from venture capital firms. This is the same stuff (other than the VC bit) that a grocery store would be doing.

To raise one source of these claims that has gone public, A16Z, a venture capital firm with multiple portfolio companies that experienced difficulty in establishing even basic banking relationships, has spoken out about this. In fact, Chris Dixon recently said on a podcast the firm literally had a full-time person to help get bank accounts for their clients¹². Olivia Chow, an incredibly talented advisor who works with me at Zero Knowledge, previously built an entire consulting practice called Yokip around getting people in crypto bank accounts. In the course of preparing for this testimony, I found no less than four crypto projects, three blockchain foundations, two stablecoin companies, and three different investment funds who all faced conditions ranging from difficult to impossible to get bank accounts or keep bank accounts, especially after the collapse of Silicon Valley Bank, Signature Bank, and Silvergate Bank. To bring you behind the curtain, this took about one day of asking around, meaning if I had three months to prepare for this testimony, I could likely bring a list 100 companies long.

On the upside, someone did have much more time: a comprehensive study has already been conducted by John D'Agostino¹³ with the AIMA, finding that a vast majority of fully legal, US-based, properly registered crypto investment funds had severe difficulties finding banking relationships¹⁴. Difficulties far in excess of much lower risk industries, you know, like hedge funds and private equity, which have plenty of access to the kinds of leverage that cause issues like Archegos or Long-Term Capital Management. In the infinite wisdom of our banking regulators, those are fine, but a blockchain foundation paying an AWS bill? Can't have that!

Again, these are not the problem children! If you think Bitcoin miners operating in the United States and selling solely through Coinbase, blockchain foundations associated with such sketchy and criminal institutions such as Stanford or MIT, or regulated New York financial services companies under the aegis of the NYDFS are "too risky" to operate in our banking system, then I have to ask some deep questions about what your definition of risk is and why any hedge fund ever, anywhere, for any reason, or any private equity firm, or, given their failure rate and the amount of money laundering risk, any restaurant¹⁵ ever has a bank account.

Equally so, the banks servicing crypto clients also found that other banks providing services to them began pulling back. Both smaller onshore banks and offshore banks have been deplatforming crypto clients because of fears over their correspondent banking relationships, and the global ecosystem is being forced into the shadow bank sector and less regulated

¹² <https://x.com/laurashin/status/1884590647547461771>

¹³ [https://en.wikipedia.org/wiki/John_D%27Agostino_\(financial_services\)](https://en.wikipedia.org/wiki/John_D%27Agostino_(financial_services))

¹⁴

<https://www.wsj.com/livecoverage/stock-market-today-dow-sp500-nasdaq-live-12-20-2024/card/majority-of-crypto-hedge-funds-report-facing-banking-issues-in-recent-years-Nat2gsEh0xPEleK6583O>

¹⁵ Much less a chain of them... or worse, franchises!

offshore jurisdictions to operate. Irony, given that in attempting to make the system more safe, this specific action virtually ensures it is actually less safe!

As if that wasn't enough, I know of a law firm that was unable to get escrow accounts because they served clients in the blockchain space, of a crypto project that was essentially destroyed by the SEC because they were having their accounts closed due to regulatory pressure but the SEC instead told a judge that they were deliberately moving money out of the country and closing accounts themselves to get a TRO¹⁶. This obviously did not end well for the SEC, thanks to some exceptional lawyering by the folks at Morrison Cohen (in particular, the indomitable Jason Gottlieb and his team), but how are we at a point where companies not convicted of any crime or wrongdoing are losing accounts because of the actions of regulators and then having businesses destroyed because Federal regulators then lie and blame the victim in court?

Perhaps most pernicious are the incidents of people having their personal accounts cancelled. If you don't believe that such a thing is possible, I would direct you to the many people who have spoken publicly about this, such as lawyers¹⁷, employees of various blockchain foundations, executives at Coinbase, and more. In some cases, it was not limited to them but also spilled over to family members and children.

This is unequivocally bad. That law-abiding citizens providing legal counsel to firms to navigate uncertain waters could have had their accounts closed for daring to, you know, practice law? That an individual could take a job in the crypto space and their young son or daughter have their beloved savings account where they are learning good financial discipline abruptly closed with no notice by a bank¹⁸? These things are deeply wrong and unamerican.

Most importantly, they happened. Before we get into the causation, all you have to do is look around the industry to find problems. Importantly, those problems afflict small companies, startups, innovators, and the politically disfavored first. Very large firms with political connections and deep lobbying benches? They probably keep their bank accounts, though with a lot of pain and annoyance. But a small startup? A minority owned firm trying to provide financial services to people outside the banking system? Someone building an idea with elbow grease to create a better block explorer to track crime?

All blocked.

¹⁶ <https://assets.law360news.com/1841000/1841579/https-ecf-utd-uscourts-gov-doc1-18316495996.pdf>

¹⁷ <https://x.com/MinarikLaw/status/1863258797323825224> &

<https://x.com/MinarikLaw/status/1886825962383511559>

¹⁸ To find a silver lining on a dark cloud, at least these children will understand why self-custody is important

The receipts are all over the VC community. You can read the AIMA study I referenced above. Or you can go talk to all the banks that wanted to serve crypto customers and were instead met with denials and intimidation.

So how did we get here?

BANK FAILURES & REGULATORY REACTIONS

In 2022, there were some problems in crypto. We had the collapse of FTX, a scam of epic proportions and in a group that includes things like Bernie Madoff and the trading scandal at Barings Bank in terms of both historical note and scale. As if that was not enough, we also had the collapse of entities like Celsius (also with criminal implications), Genesis (still ongoing as to the exact implications) and through them DCG, BlockFi (perhaps not criminal but certainly quite dumb), 3AC (wildly criminal and it remains shocking to me charges have not been brought in the United States), and TerraForm Labs, the ill-fated issuer of the “stable” coin UST.

It wasn’t great! People did lose vast sums of money, and the financial devastation was real.

As a result of this, a number of actions were taken by banking regulators, and here is where the picture gets muddy, which is why I want to describe in at least some detail the events which occurred.

First, two of the major crypto-constructive banks were shut down: Silvergate was subjected to significant regulatory pressure and, allegedly, verbal guidance from banking regulators (particularly the FDIC) that made its core business impossible to operate. The bank went into voluntary liquidation in March of 2023 and later paid a \$63mm settlement relating to charges of insufficient controls around anti-money laundering and financial crime in 2024¹⁹. Signature bank was also shut down in March of 2023 by the New York Department of Financial Services and the FDIC was appointed as the receiver, with these actions taken because of risk to the overall financial system, or at least language used by regulators and government officials indicated that²⁰. In the Signature case, the FDIC process was initiated on a Sunday (unusual, given Friday was typically when these actions occurred in the past) and the bidding was highly confidential²¹, also unusual given the alleged sequestering of the digital assets and also alleged rejection of bids for Signet, the banks 24/7 real-time settlement platform for internal settlement of deposits between customers (e.g. two customers of Signature bank could interact at 3am on a Sunday, something patently impossible through Fedwire or some such, given we insist on living in the 1980s technologically in the U.S. banking system).

¹⁹ If you think that is bad, hold onto your hat and keep reading

²⁰ <https://www.reuters.com/business/finance/new-york-state-regulators-close-signature-bank-2023-03-12/>

²¹ <https://www.theracetothetbottom.org/rttb/2023/7/7/signature-bank-failed-are-more-us-banks-next>

I separate these two banks from Silicon Valley Bank because Silvergate and Signature handled significantly more customer money and provided 24/7 real-time settlement platforms, something essential for crypto given that blockchain rails function 24/7 and traditional banking rails function ~30% of the time from a calendar hours basis²². There is functionality they provided to the crypto industry, facilitating the majority of flows for stablecoins and exchanges, that was shut down and essentially not replaced.

Second, there was the collapse of Silicon Valley Bank. SVB was closed on a Friday in March, and shut down shortly thereafter and sold off. Here, the cause of the collapse was a pretty traditional bank run: they didn't have enough money to pay back all the depositors who wanted their money back, because they had gone into very long duration bonds while interest rates went up²³. Having a concentrated depositor base in the tech sector paired with a very illiquid loan book would have been the kind of thing I advised people to not do when I was back at JPM. Here, it ended badly for exactly the reasons one might expect such a thing to end badly.

That is a factual description of things that happened and banks that collapsed, but to understand the spiraling web of regulatory actions behind it, we have to look at least one layer deeper.

Namely, through FOIA²⁴ requests, Coinbase has uncovered that the FDIC in particular had been rattling the cage with banks²⁵ with varying degrees of specificity, across a broad variety of programs. Some of these objections are likely valid (you don't want banks lending in risky fashion against highly volatile crypto assets), some of these objections seem less valid (offering investment products with risks disclosed and off the bank's balance sheet seems... strange... to object to), and some of these objections just seem like wild overreactions at best to actively malicious at worst (banking crypto clients at all).

More so, through conversations with staff, executives, and former personnel at over 10 different banks who banked crypto clients so that I could assess banking activity myself, I was told repeatedly that the FDIC was delivering verbal guidance far in excess of what they were putting in writing. These have included rumors of FDIC demands such as a 15% cap on crypto deposits²⁶ no matter the matching assets, a requirement to get regulatory approval to open accounts for any crypto clients or engage in any new activity in or adjacent to the space (which was never given),

²² I will gently remind everyone that countries like Japan and South Korea have had 24/7 real-time bank settlement since the early 2000s, so this is a choice to freeze our technology at a specific point in the time and reject progress in the United States by our banking regulators, like a financial version of the Amish

²³ Surprisingly for a college professor, there was a method to my madness explaining how banks work

²⁴ I sent the FDIC a FOIA request asking if they have been monitoring and coordinating against critics, naming specific individuals and timeframes, and they are refusing to answer me because it is "overbroad" despite the specificity, just to show how difficult it is to hold them accountable

²⁵ <https://x.com/iampaulgrewal/status/1875226182662418471>

²⁶ Please refer back to my previous comment on the Miata - 15% crypto deposits backed by t-bills or reserves at the Fed would be very different than such deposits backed by 30 year real estate loans

and constant questions and examinations around any crypto activity designed to intimidate banks into deplatforming clients.

Adding credence to this behavior, the banking regulators have put out multiple²⁷ letters²⁸ about crypto²⁹ that contain, when pulled out, some interestingly confusing and self-contradictory statements:

“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.”

“In the statement, the Board also reiterates to state member banks that legal permissibility is a necessary, but not sufficient, condition to establish that a state member bank may engage in a particular activity.”

“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.”

“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.”

“The Board generally believes that issuing tokens on open, public, and/or decentralized networks, or similar systems is highly likely to be inconsistent with safe and sound banking practices. The Board believes such tokens raise concerns related to operational, cybersecurity, and run risks, and may also present significant illicit finance risks, because—depending on their design—such tokens could circulate continuously, quickly, pseudonymously, and indefinitely among parties unknown to the issuing bank. Importantly, the Board believes such risks are pronounced where the issuing bank does not have the capability to obtain and verify the identity of all transacting parties, including for those using unhosted wallets.”

This, to avoid sugarcoating it, is an absolutely radioactive tire fire with regard to guidance.

Our banking regulators have clearly stated that banks are not prohibited from providing services to the crypto community legally, but also clearly stated that legal permissibility does not mean they are allowed to provide services³⁰.

They have stated that banks with sufficient controls are permitted to serve this industry, but also that it’s unlikely there are even sufficient controls they feel are possible, and that they are going to address this on a case-by-case basis with no consistency so that such standards are unlikely to be developed.

²⁷

<https://www.federalregister.gov/documents/2023/02/07/2023-02192/policy-statement-on-section-913-of-the-federal-reserve-act>

²⁸ <https://www.fdic.gov/sites/default/files/2024-03/pr23002a.pdf>

²⁹ <https://www.fdic.gov/news/financial-institution-letters/2023/fil23008a.pdf>

³⁰ <https://www.reactiongifs.com/wp-content/uploads/2013/10/tom-delonge-wtf1.gif>

Lastly, they remind everyone that banks are responsible for the conduct of users once money is off their platform, a standard they do not apply elsewhere in the banking system (e.g. JPM originating a deposit that a customer then sends to another bank does not make JPM liable when the receiving entity has another customer with those funds who then commits fraud unrelated to the JPM transaction), which helpfully is a thing you definitionally can't control for or report on.

Importantly, much of this is also largely untethered from the specific concerns about keeping banks well capitalized and operating³¹. "Reputational risk" and amorphous concerns about anti-financial crime are not reasons that banks fail. In fact, the latter is precisely the justification used for the racial discrimination of redlining: because this group of people has some criminals and/or non-creditworthy people, rather than doing individualized analysis, we're just going to block the entire group. I am deeply opposed to this on moral grounds, and in fact the excessive compliance costs created by this behavior probably falls most strongly on minority communities and politically disfavored groups.

I will also remind everyone here that the FDIC in particular uses a system called CAMELS to rate banks, and the "M" in CAMELS stands for management. This is a completely subjective category, so it creates the following tautology: if the regulator thinks a space is risky for unclear or inappropriate reasons, then management thinking that space is good for a bank will be downgraded, damaging their score and imposing penalties like higher FDIC charges or even up to and including prohibitions on onboarding new customers or having your charter revoked. In short, because a regulator can deeply penalize a bank for "bad judgment", with bad judgment meaning anything the regulator subjectively does not like, guidance that implies a space is very risky is tantamount to guidance that if you do it, the M score in CAMELS will go down. A lot.

If you are a bank, what are you supposed to do with this guidance? I can tell you what I would have done when I was running trading desks at JPM and Citi: I would have assumed it was prohibited.

Importantly, I don't mean prohibited in the sense that I can't. I mean prohibited in the sense that if I do it, there will be such severe financial and procedural penalties that it will slowly grind my bank into dust. You'll be subject to operating risk capital increases. You'll be subject to higher FDIC charges. You'll be investigated constantly and forced to quintuple your compliance budget. You'll just have your time constantly wasted as \$2.71 transactions to buy a coffee are scrutinized to make sure you did KYC and anti-money laundering, politically exposed person, and OFAC checks before letting someone process that payment.

³¹ More on this later in the How Banks Work section

In short, the process is the punishment, and the regulators and the banks both know it. No one in their right mind is going to deliberately put a commercial enterprise in that situation, especially when they answer to shareholders.

As a result of this “guidance”³², banks started closing the accounts of crypto companies left and right for non-financial reasons. The message was received. Basic checking accounts, for those amorphous “reputational risk” reasons were being closed. Threats of constant examinations and AML/KYC fines were made against banks serving crypto (while, helpfully, regulators ignored or took a full decade to act on much worse conduct in the traditional financial system³³, possibly because these resources were instead being misdeployed into intimidating jpeg artists out of having bank accounts). In short, banks mostly concluded it was too hard to serve the industry, so they didn’t. This sort of jawboning to intimidate banks is even going on today³⁴, with Fed Chair Jerome Powell recently stating at a press conference that “Banks are perfectly able to serve crypto customers, as long as they understand and can manage the risks, and it’s safe and sound,” and then hilariously went on to say the bar was higher for crypto risks and while the Fed was not against innovation, crypto was scary and should be viewed with deep skepticism.

Full disclosure: I am a parent, and I have two children, ages 9 and 5. More than once, I have told them “you can do this but I wouldn’t, if I were you” and I understand exactly what that means and so do they: you’re about to get in trouble if you do this. Banks understand this is what the regulators are saying when Powell says things like this, too.

When you combine that with the shutdown of the most crypto friendly banks, here is the situation that most crypto companies faced: the banks, which were the most risk-tolerant of novel technologies, are being shut down and can’t bank you anymore, so you have to find a new bank. However, the joke is on you: there are no new banks who want your business, and if they take it, the regulators will try to find a way to shut them down too.

Why is this, though? You may recall that many pages earlier, I said that deposit accounts of the sort that are being denied here are some of the most profitable.

Here is where we get to the problem of AML/KYC and reputational risk. While it is beyond the scope of this hearing, an overall comment I would make is that the AML/KYC regime is incredibly effective at producing paperwork and incredibly ineffective at actually stopping financial crime. This is because there are no real effective measurements of the traditional financial system on this basis, because it is opaque, fragmented, and nobody has a holistic look at the information

³² By which I mean thinly veiled threats

³³

<https://www.justice.gov/opa/pr/td-bank-pleads-guilty-bank-secrecy-act-and-money-laundering-conspiracy-violations-18b>

³⁴

<https://www.thestreet.com/crypto/policy/fed-chair-powell-calls-on-congress-to-create-regulations-around-crypto>

What that does is put each bank in a situation where perfection is impossible, so if a regulator wants to use AML concerns as a pretext to engage in things like illegal discrimination based on speech to harm private individuals, they can do so. Similarly, if you want to punish a bank, you can find them guilty of AML violations essentially all the time.

This is not to discount the very real problem of financial crime, but rather, this is a statement that the rules seem calibrated to create paperwork and fines, not solve the problem.

Reputational risk is an even more amorphous concept. It is the idea that somehow the reputation of a bank could be damaged, making it less likely that it can continue as an ongoing concern and that depositors would flee because...? It's unclear what this really means, because in practice it appears never to have sparked a bank run, but rather is a tool for regulators to use to force the debanking of industries they don't like, or for banks to eject customers they don't want, but without having to bother with all of the nonsense about actually having business-relevant reasons, valid risk concerns, or those customers having to have actually committed some wrongdoing. No, it's more like "that customer wore the wrong shirt, and we don't want our reputation associated with the kinds of horrific monsters who think it's okay to wear orange, so you are gone" behavior in practice. When a single bank does that for idiosyncratic reasons, that's actually not a big deal. When the entire industry does it to a sector because regulators hate orange shirts, suddenly every Cleveland Browns fan can't get a bank account. If you don't believe that, go re-read the part on how CAMELS scores work and realize that being in a reputationally risky space is a reason to dock a bank's management score.

Maybe unsurprisingly, in the documents quoted above, regulators said that crypto has heightened reputational risk. Who could have seen it coming that a poorly defined category based on subjective bias would be used against politically disfavored industries or people?

LIVING WITHOUT A BANK

In preparing for this testimony, I've started to try to figure out just how essential banks are to our lives in 2025. It wasn't always like this. My grandfather used to tell me about how he'd pay for almost everything in cash, and the only thing he really needed a bank for was buying a house or maybe a car. Now, thanks to electronic payments, I can barely buy a coffee without a bank being involved somewhere, somehow.

In the past few days, I have tried to figure out if I could personally pay any of the following using cash, or failing that, with some method that would not require me to explicitly touch a bank:

- Amazon will give me options for debit cards, credit cards, HSA/FSA, and Amazon store cards, which means cash is out.
- My condo dues can be paid with a debit card, credit card, or ACH. No cash.

- My car insurance was also a no. When I called GEICO to ask if I could mail them cash, the person on the phone sounded mildly panicked³⁵ until I explained it was just for research.
- My New York City property taxes are potentially a yes. Online I can only pay with the usual mix of cards and bank accounts, but I can theoretically pay in person if I'm willing to travel to the office in person, which appears to be a roughly 30 minute trip in each direction plus the time it would take to have the appointment³⁶, and involve carrying many thousands of dollars in cash around in person.
- Getting paid by NYU, to which the answer was, to summarize, "absolutely not" and also "stop it". At most they will mail me a check, which I could take to a check cashing location, pay an absurd fee, and then end up with cash. After the 7 business days it takes to get mailed the check, assuming it is not stolen out of the mail.
- Buying food at the local deli or grocery store, which was one of the other rare success stories and they were happy to accept cash.
- Finally, could I buy stocks with cash? Robinhood conclusively told me no.

So what can I do with cash in any timely fashion? Buy food and pay my property taxes.

What can't I do? Have a condo³⁷, have car insurance, have a job, buy anything from Amazon.

The good news is that I have food! The bad news is that I'm homeless and unemployed.

I will note that for some of these, there is a backdoor to cash through something like PayPal or CashApp or Coinbase, if I get the money into them through an ATM, after paying fees, and then transfer that money in tiny amounts to certain platforms or use a debit card linked to those accounts. Again, there is a bank under there somewhere, though I may not explicitly have an account with said bank. Equally, in some of these cases (like property taxes), I could operate with cash, but the deadweight cost of having to spend large amounts of time means it is vastly less efficient and would be incredibly disruptive to someone working a job (or multiple jobs) or with childcare or elder care responsibilities. This is before we get to the incredible fees for things like check cashing (and having to do that in person, also taking time).

Being without a bank account, personally, means that you are unable to interact with significant parts of electronic commerce, and for other parts, while you can interact in person, your explicit and implicit costs are vastly higher than someone with a bank account. As always, the poor and already marginalized suffer the most from lacking these services as a result.

We're not even done yet. You may notice that above, I asked about my personal bank account. I also tried to figure out if Zero Knowledge could operate without bank accounts.

³⁵ Asking experimental questions that cause some degree of panic, confusion, or immediate consternation seems to be an essential part of being a professor, for anyone considering it as a career

³⁶ <https://www.nyc.gov/site/finance/about/contact-us-visit-brooklyn.page>

³⁷ Astute readers will note this renders the property taxes part irrelevant

In short: no.

Any corporate entity would not be able to do tax withholding properly for paying employees if we are delivering solely cash without doing it manually and then somehow figuring out how to pay the IRS and state agencies. Paying filing fees for licenses is going to be rather difficult, and that's before we get to having to post bonds for capital for some financial activities involving handling money, often required for certain financial businesses. Paying rent? Vendors? Internet service providers? Cell phone service? Web hosting? D&O insurance?

You rapidly go down a rabbit hole where the majority of things that you need to run a business are simply unavailable to you when you operate only with cash.

What this means is that if you are debanked, you cease to have a traditional business. You could maybe have certain types of fully remote Web3 or tech businesses, but it's going to be far more difficult (perhaps not impossible, but with major limitations on scalability, business model, and customers) in a way that ranges from limiting to crippling to immediate bankruptcy. It's always damaging.

AMERICA LOSES

One of the biggest losers here is America itself. This sort of embargo against an entire legal industry, either through active malice or incompetence, is the sort of thing that sticks in the mind of entrepreneurs. I will point out that vast amounts of venture capital funding, many very well-compensated jobs in the tech sector, and significant amounts of dollar flow in investment products are all outside of the United States because of this action. As of the time of the writing of this testimony, the total market capitalization of the crypto space is over \$3.6T as per Coin Gecko (yes that's the real name), untold billions in crypto funding have been employing people all over the globe except here³⁸, and the reputation of American regulators and financial markets as fair and impartial have been damaged.

A good example of this is in the stablecoin space. Stablecoins are the representation of a dollar on a blockchain, and the overwhelming majority of them do this by having actual dollars in a bank account or short-term, high-quality investments held with custodians. Where is the largest stablecoin in the world, Tether, based? El Salvador, soon! Again, this is a \$139B dollar investment pool, representing one of the largest buyers of treasuries in the world, and they want absolutely nothing to do with the United States, which also deprives us of all their customer data.

³⁸ Also probably not Iran, North Korea, or a few others

What other jurisdictions are launching stablecoin frameworks? Europe, with the barely workable framework in MiCA that is mostly being ignored, but also Hong Kong, Singapore, and the United Arab Emirates.

Let me say that again: it is entirely possible that the number one location for global stablecoins in ten years, on the current pathway, is literally going to be Hong Kong, meaning that control of the blockchain dollar system and every single scrap of customer data related to it will be in the hands of China rather than the United States.

This seems kind of insane, doesn't it?

The fact that this story could repeat for other industries, over and over, because of these governance and structural problems is itself a dire threat to national security. Accidentally or purposefully forcing an emerging financial technology offshore because some out-of-touch bureaucrats in a banking regulator privately threatened banks and neither the President nor Congress knew exactly what was going on is exactly the kind of thing you would expect in a dysfunctional autocratic regime, not the United States of America, where we are supposed to be the gold standard of representative and transparent government globally.

I would suggest we can (and should) do better.

REFORM

What we need are reforms to ensure that this sort of activity, deliberate or merely cruelly indifferent, stops happening to law-abiding American citizens and businesses. It has already happened twice. That is enough. To that end, I would propose the following, in order of priority, to Congress:

First, all banking supervisory guidance should be required to be in written form. No more verbal guidance³⁹. That guidance should also be made public, completely unredacted except for the names of private individuals, on a 12-month trailing basis. There is no issue so severe that a bank given a full year head start cannot remediate it to the point it is not critical if it becomes public, or if such an issue does exist, the bank should just be shut down.

Second, when a bank debanks someone, they should be required to say why. This is important to create a paper trail, and given banks have a monopoly on certain types of economic activity granted to them by our laws, it is not unreasonable to ask that they explain themselves truthfully. This need not create a pathway to appeal of the decision, and the only criteria should be that it is

³⁹ Delivering verbal guidance that is not documented in written form should lead to immediate termination of the staff involved and personal liability for those staff

both truthful and provides a clear articulation of the reason⁴⁰. The importance is creating the record so we can see when, where, how, and why people are being debanked.

Third, reputational risk as a risk factor to be considered by regulators should be strictly prohibited, and management as a component of CAMELS should either be removed or greatly reduced in impact. This is all too easily used as a cover for things like illegal discrimination on the basis of race, as retaliation for first amendment protected speech, and more. The amorphous and poorly defined nature of "reputational risk" or "management" is ripe for abuse, and it should be prohibited.

Fourth, all supervisory guidance should be subject to a balancing test weighing the harms the regulations are attempting to prevent against the impact the regulation is having on banking access for law-abiding Americans. Importantly, this evaluation should not be done by the agency itself, but rather by an outside arbiter. I would suggest 3 months, 1 year, and 5 years as appropriate milestones for review to track impact over time, and if the outside arbiter finds that a regulation is poorly designed and doing more harm than good, it is negated.

Fifth, there should be a rule that banking supervisory guidance and rules should apply equally to all institutions. No more case-by-case handling or privately playing favorites or punishing institutions. Clear rules and criteria for compliance should be required.

Sixth, I would suggest that firms or persons that are debanked due to excessive regulatory animus or impermissible motives (such as speech discrimination) and themselves have not been charged with any criminal acts should have a private cause of action against the banking regulators. As I described much earlier in this document, banking access is essential for modern life and confidential revocation of it could easily be used as a tool of illegal discrimination against Americans. The victims should be able to defend themselves.

These reforms together would primarily fix the governance around banking regulation, preventing banking regulators from being judge, jury, and executioner and also exposing their processes to the light of day and public scrutiny. While it will not fix all of our issues, it will at least create the structure needed to address them in the future and prevent further incidents where secrecy is used to hide bad intentions or poor conduct.

I will end with the statement that I believe enacting reforms to prevent this activity in the future is growing increasingly important each time this sort of incident occurs. If we ignore it and enshrine the principle that, so long as they adequately cloak their motives in confusion and are clever enough not to write down the bad bits, regulators answering to the executive branch can debank entire industries or groups just because they don't like them, where are we going to end up as

⁴⁰ If that reason is that regulators are making the compliance costs too high or threatening banks with harm for banking that client, they should be able to just say that

this cycle continues? I hope we are wiser than to explore that particular future path, and instead put an end to these practices now.

Thank you.

Chairman MEUSER. Thank you, Mr. Campbell.
Mr. Grewal, you are now recognized for 5 minutes for your remarks.

**STATEMENT OF PAUL GREWAL, CHIEF LEGAL OFFICER,
COINBASE GLOBAL, INC.**

Mr. GREWAL. Chairman Meuser, Ranking Member Green, and distinguished members and staff of the committee, thank you for the opportunity to testify today. My name is Paul Grewal, and I serve as the Chief Legal Officer at Coinbase, the largest publicly traded crypto company in the United States.

Today I want to shed light on the systematic effort to debank the American crypto industry, and then to deny it the legal protections afforded by Congress and the courts. While crypto is the current target, any legal American industry could be next if regulators continue to use banking services as a political weapon. My focus today is on the actions of the FDIC.

In March 2022, the FDIC began sending letters to senior bank officials urging them to stop all crypto-related activity with no clear timeline for review, or for sharing any analysis of explicit risks. The letters continued well into 2023. In October 2023, the FDIC's own inspector general issued a report making clear the FDIC was actively limiting financial innovation with little regard to actual risk to the financial system.

That Inspector General (IG) report recommended the FDIC establish a plan with time frames for assessing crypto-related risk and clarifying the supervisory feedback process regarding crypto activities. The FDIC agreed to implement these recommendations by January 2024, but more than a year later, the FDIC did not implement anything and still has not implemented anything that adequately addresses these problems.

We agree regulators should assess financial risks, but they should not use political bias to stifle a legal industry behind closed doors. As a result, Coinbase and our partner filed multiple Freedom of Information Act (FOIA) requests to the FDIC to uncover the extent of their actions. After the FDIC stonewalled us at every turn, we sued in the Federal District Court in order to obtain the information.

The court ordered the FDIC to release redacted versions of their pause letters. The FDIC's initial production, however, was threadbare, but, just yesterday, as Mr. Campbell indicated, and at the direction of FDIC Acting Chairman Hill, the FDIC finally released a more complete set of 175 documents, totaling over 700 pages that revealed an even more disturbing pattern and practice to debank our sector than previously known.

Over and over again, the FDIC bludgeoned the banks with an onslaught of examinations and questions until the banks relented under the pressure. For example, the documents show that regulators forced banks to deny stablecoin issuers bank accounts for the reserves. That meant stablecoin issuers had fewer places to turn for banking services causing increased concentration risk and fewer opportunities for community banks and others to grow deposits.

In this very room, policymakers have raised concerns that crypto could pose a risk to the traditional financial system, but because

of the FDIC's actions, here the opposite happened. The traditional financial system posed a risk to crypto and critically its customers.

During the same period in which the FDIC was telling banks to halt activity, the FDIC was also publicly denying they were discouraging banks from offering services to lawful businesses, including crypto. For example, in a January 2023 joint statement, the FDIC, along with other banking regulators, explicitly stated that 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.

Regardless of one's views on crypto, everyone should be alarmed that regulators were saying one thing publicly while instructing banks to do something very different behind closed doors.

Coinbase's FOIA litigation has exposed this lack of transparency, regulatory bias, and abuse of power. Bringing these issues into public view has significant implications not just for crypto, but for broader regulatory fairness.

I remain optimistic about crypto's future in America despite the abuse I have outlined today. We can start by enabling banks to provide crypto services to all lawful businesses. To that end, Coinbase sent a letter to the banking regulators earlier this week urging them to take specific actions like withdrawing the Office of the Comptroller of the Currency (OCC) Interpretive Letter 1179 and enabling innovative technology solutions.

In addition to opening up banking services to the crypto industry, I would urge Congress to pass legislation that creates regulatory, certainly for crypto. I applaud the work of Chairman Hill and other members of this committee for their work on Financial Innovation Technology for the 21st Century Act (FIT21) and stablecoin legislation, and we are eager to engage on similar legislation this year.

Thank you, and I look forward to answering your questions.

[The prepared statement of Mr. Grewal follows:]



Testimony of Paul Grewal
Chief Legal Officer

Before the U.S. House Committee on Financial Services
Subcommittee on Oversight and Investigations

Thursday, February 6, 2025

Chair Meuser, Ranking Member Green, and distinguished members of the committee:

Thank you for the opportunity to testify today. My name is Paul Grewal, and I serve as Chief Legal Officer at Coinbase, the largest publicly traded cryptocurrency company in the United States.

Today, I want to shed light on the systematic effort to debank the American crypto industry, and then deny it the legal protections afforded by Congress and the courts. While crypto is the current target, any legal American industry could be next if regulators continue to use banking services as a political weapon. This attack on banking services spans multiple agencies and dates back more than four years.

I am going to highlight the actions of one particular agency, the FDIC. As I will explore, as early as March 2022, the FDIC began sending dozens of letters to senior members of financial institutions directing them to “pause all crypto asset-related activity” regardless of type or materiality with unspecified timelines for agency review.¹ In April 2022, the FDIC formally required that these institutions self-report any proposed crypto-asset activity, again regardless of type or materiality.² In January 2023, it obfuscated these efforts by joining other regulators in declaring that “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.”³ And in October 2023, in response to a finding by its Inspector General that it had, to date, completed no crypto-asset risk assessments or provided any timelines for reviewing any identified crypto activities, it committed to finally doing so in less than six months.⁴ Eighteen months later, no such assessments or timelines have been publicly identified.

This attack illustrates a fundamental issue that transcends the debate over cryptocurrency: the lack of transparency and accountability in regulatory practices. Although some may argue that regulators should assess whether engaging in crypto-related products and services could impact a bank’s safety and soundness, this should not justify allowing anti-crypto bias to hinder a legal industry. Rather than starting with the assumption that engaging in crypto is inherently problematic, regulators should approach the issue openly, with the goal of identifying practical solutions and promoting innovation. I will close my testimony with proposals that will help reverse the debanking trend of recent years, and open up banking services for crypto to financial services companies and crypto companies alike.

¹ Appendix C, *History Associates Inc. v. FDIC*, No. 1:24-cv-1857-ACR (D.D.C.) (“FDIC FOIA Litigation”), Docket Entry 27-2, March 11, 2022 FDIC Pause Letter.

² FDIC, Financial Institution Letter (FIL) 16-2022, *Notification of Engaging in Crypto-Related Activities* (issued April 7, 2022), <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html#letter>

³ Federal Reserve, FDIC, and OCC, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 3, 2023), available at <https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf>.

⁴ Appendix A, FDIC Office of Inspector General, *FDIC Strategies Related to Crypto-Asset Risks* (Oct. 2023) (“OIG Report”), pp. ii-iii, <https://tinyurl.com/3kudyxyn>.

Background on Coinbase's Experience

Coinbase has always operated with a commitment to compliance, transparency, and innovation. We educate policymakers, regulators, and the public on cryptocurrency, advocate for diversification in financial services, and aim to build a future where financial systems work better for everyone. Founded in 2012 in the United States and publicly listed on the NASDAQ in April 2021, we have grown to serve millions of users across over 100 countries, offering a secure and user-friendly interface for both retail and institutional investors. We are committed to building an open financial system for the world and operate with strong regulatory compliance, security protocols, and innovative features to ensure a seamless and trustworthy user experience.

Coinbase is currently regulated by more than 50 regulators in the U.S. alone: we are a money services business registered with the US Treasury Department and subject to Financial Crimes Enforcement Network (FinCEN) rules, and we have served on the Department of the Treasury's Bank Secrecy Act (BSA) Advisory Group. We have 45 state money transmission licenses, and a BitLicense and state trust charter from the New York Department of Financial Services (NYDFS). We are a licensed designated contract market (DCM) and a futures commission merchant (FCM) regulated by the CFTC, and Coinbase Asset Management is a registered investment advisor under the SEC. Internationally, we are also subject to regulatory supervision in a number of markets, including the United Kingdom, European Union, and Singapore; these regulators also have a heavy focus on financial crimes and mandate implementation of strong AML programs.

Despite our commitment to regulation and growing the American crypto economy in a safe and responsible way, over the past two years we have witnessed and encountered unprecedented challenges from coordinated regulatory actions that seek to paralyze cryptocurrency. These efforts often took place in the shadows, without the benefit of public awareness, input, or debate. As a publicly-traded company with strong bank partners who are willing to engage with our team on important due diligence questions and better understand how Coinbase operates, we have been successful in managing the attack. But many others with far fewer resources have not been so fortunate.

Coinbase takes seriously our obligation to help fight for the future not just for ourselves, but for the entire crypto economy. Over the last two years, Coinbase has heard stories of both crypto companies and employees who have been victims of debanking. They are compelling and powerful, and it spurred us to act.

In light of this unprecedented assault on an entire industry, Coinbase took the unusual step of not only filing Freedom of Information Act (FOIA) requests in relation to these inappropriate regulatory actions, but also suing the regulators in court when they stonewalled us.

The Players and the Campaign Against Crypto

To understand the scope of this campaign, it's important to identify the key players and tactics:

- **Regulators:** In response to executive orders, policy shifts, and joint statements, the FDIC and other regulators have taken a decidedly hostile stance toward crypto.
- **Banks and Financial Institutions:** Banks have been pressured behind closed doors to halt any crypto activities (including facilitating basic Bitcoin transactions), and sever ties with crypto companies, limiting their access to essential financial services.
- **Crypto Companies, Employees, and Investors:** The resulting regulatory uncertainty has disrupted businesses, displaced employees, and created unnecessary risks for millions of Americans.

Defining Debanking

Debanking is not a new concept in the United States and refers to the practice of financial institutions denying or restricting access to banking services like opening accounts, processing transactions, and securing loans to individuals, businesses, or entire industries. Historically this has happened for regulatory, political, or reputational reasons, even if the affected entity is operating legally.

In the case of the crypto industry, debanking has occurred in recent years due to banks and financial regulators systematically limiting or cutting off crypto-related businesses from essential banking services. This activity has included:

- **Account closures or denial:** Banks refusing to open or maintain accounts for crypto companies.
- **Restricted services:** Limiting access to payment processing, loans, or wire transfers.
- **Regulatory pressure:** Agencies like the FDIC, SEC, or Federal Reserve – as we have noted and will explore further – discouraging banks from working with crypto firms through informal guidance or behind-the-scenes influence.

Debanking has historically been used against politically sensitive industries, such as firearms and cannabis, and is now being leveraged against crypto firms, potentially setting a dangerous precedent for other industries.

Timeline of FDIC Actions to Debank Crypto Companies

The FDIC regulatory attack on crypto started as early as March 2022 by putting pressure on financial institutions to refuse banking services to crypto companies, refuse to expand services and products for existing clients, fully suspend services and products for existing crypto customers, and lock down their own internal blockchain activities.

1. **FDIC “Pause Letters” (March 2022):** The FDIC started sending confidential “pause letters” to banks, instructing them to cease engaging in crypto-related activities, including facilitating basic Bitcoin transactions. These letters, which targeted senior executives, effectively forced financial institutions to halt crypto-related projects and partnerships with crypto companies without clear explanations or timelines for reassessment.

2. **Banking Regulators Publicly Denied Discouraging Banks From Providing Banking Services of Any Type (January 2023):** The Federal Reserve, FDIC, and Office of the Comptroller of the Currency (OCC) issued a joint statement warning banks about the risks of engaging with cryptocurrency companies. But mindful of the absence of any legal authority to issue any blanket ban and, in direct contradiction with the pause letters the FDIC was sending, the joint statement said that “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.”⁵ Many financial institutions began severing ties with crypto businesses out of fear of regulatory repercussions.
3. **Inspector General Report (October 2023):** After reviewing the FDIC’s strategies related to crypto-asset risk, the Office of Inspector General found that “the FDIC has not yet completed a risk assessment to determine whether the Agency can sufficiently address crypto-asset-related risks through actions such as issuing guidance to supervised institutions. In addition, the FDIC’s process for providing supervisory feedback on FDIC-supervised institutions’ crypto-related activities is unclear.” Rather than dispute these findings, the FDIC concurred with both report recommendations to correct these deficiencies, with a committed plan to do so by January 30, 2024.⁶
4. **Congressional Request and Lack of Response (2023):** Members of Congress sought transparency from regulators, sending a letter⁷ requesting clarification on regulatory actions affecting crypto companies. This letter received no substantive public response, leaving critical questions unanswered. The lack of engagement from regulators fueled concerns about the opacity and bias of the regulatory process.
5. **Coinbase FOIA Litigation (2023–2024):** Coinbase and others filed FOIA requests to uncover the rationale behind regulatory actions targeting the crypto industry. However, these requests were met with intense resistance, stonewalling, and excessive redactions. Court interventions were required to force the release of information, exposing a troubling reluctance by regulators to operate transparently.

Coinbase’s FOIA Request

Coinbase Files FOIA Requests to Uncover Anti-crypto Debanking Efforts

At Coinbase, we believe in the necessity for fair regulations in the cryptocurrency industry. In fact, we have gone to court to fight for rules for crypto and have urged Congress to pass crypto legislation on market structure and stablecoins.⁸ Critical to any effective regulatory scheme is responsible regulatory oversight. In October 2023, the FDIC’s own Office of Inspector General Report criticized the FDIC for “limit[ing] financial institution innovation and growth in the crypto

⁵ Federal Reserve, FDIC, and OCC, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 3, 2023), available at <https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf>.

⁶ Appendix A, OIG Report, pp. ii-iii.

⁷ Letter to Prudential Regulators Regarding Efforts to De-Bank the Digital Asset Ecosystem. Reps. McHenry, Hill, <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408737>

⁸ Testimony by Paul Grewal, House Agriculture Committee, June 6, 2023. <https://docs.house.gov/meetings/AG/AG00/20230606/116051/HHRG-118-AG00-Wstate-GrewalP-20230606.pdf>; *Coinbase, Inc. v. SEC*, No. 23-3202, 2025 WL 78330 (3d Cir. Jan. 13, 2025).

space” by sending confidential letters asking financial institutions to pause ongoing or new crypto-related activities.⁹

The report found that “the FDIC has not yet analyzed the crypto-asset risks and documented its assessment of them. Specifically, the FDIC has not assessed their significance in order to determine the magnitude of impact, likelihood of occurrence, and nature of the risks. Also, the FDIC has not developed mitigation strategies, such as issuing guidance to financial institutions, to ensure that risks are within the defined risk tolerance.”¹⁰ The report also noted that “if the FDIC does not assess the significance of the risks posed by crypto assets, it might not take appropriate actions to address them. The FDIC should conduct risk assessments as a basis to develop mitigation strategies. Without a risk assessment, the FDIC may not develop and issue effective policies, procedures, and guidance to address these risks. If the FDIC does not provide its supervised institutions with effective guidance, the FDIC and some FDIC-supervised institutions may not take appropriate actions to address the most significant risks posed by crypto assets. This could impact the FDIC’s mission to promote financial stability.”¹¹

All this made clear that these closed-door, anti-crypto efforts had reached a point that could no longer be tolerated. Coinbase, through a company known for its FOIA expertise, filed multiple FOIA requests with the FDIC and other government agencies to shed light on this conduct. FOIA is a foundational tool enacted by Congress to promote transparency and accountability in government. Importantly, FOIA is the law that allows the public to request access to federal agency records, including documents that illuminate government decisions and operations, unless they are exempt by law for reasons such as national security or personal privacy. What we have learned through these FOIA requests about the FDIC’s efforts to pressure financial institutions, and from the FDIC’s own conduct in attempting to prevent this information from coming to light, has been particularly troubling.

After we filed a FOIA request with the FDIC in November 2023 asking for copies of all the ‘pause letters’ described in the Inspector General’s Report, the FDIC denied the request in full by attempting to hide behind the supposed application of FOIA exemptions based on supposed claims of “confidential supervisory information,” apparently without searching for those documents or considering whether they could be provided in redacted form. We then brought an administrative appeal of that finding, explaining that even if FOIA exemptions applied to part of these pause letters, there must be some material that could be provided in redacted form, consistent with FOIA’s principles of transparency and respect for the FDIC’s interests. But the FDIC doubled down and denied our appeal in full, again inappropriately hiding behind broad claims of confidential supervisory information.

Coinbase Sues the FDIC in Federal Court for Violating FOIA

In June 2024, Coinbase sued the FDIC in federal district court for violating FOIA by entirely withholding the pause letters. The FDIC continued to resist disclosing a single word of any

⁹ Appendix A, OIG Report, p. 13.

¹⁰ *Id.* at p.10.

¹¹ *Id.* at p.10.

pause letter, claiming without specificity that disclosure would harm banks and the agency. We argued to the court that the FDIC should be able to provide the pause letters in redacted form in a way that shields the names of particular banks and other legitimate confidential supervisory information. The court agreed, and in September 2024, instructed the FDIC to provide within 30 days the pause letters with appropriate redactions. Thirty days later, the FDIC inexplicably did not provide any pause letters. After Coinbase brought this to the court's attention, the court reinforced its prior order and required the FDIC to make redactions and produce the pause letters.

In November, the FDIC provided highly redacted versions of the pause letters, leaving unredacted a smattering of words with little substance, making them nearly incomprehensible.¹² At Coinbase's request, the court itself reviewed the unredacted versions of some of the pause letters and was far from satisfied. The court ordered the FDIC to "re-review the documents" and "make more thoughtful redactions."¹³ The court explicitly stated that it was "concerned with what appears to be FDIC's lack of good-faith effort in making nuanced redactions" and said that the FDIC "cannot simply blanket redact everything that is not an article or preposition."¹⁴ As a former federal magistrate judge, I know that words like these carry great weight.

The Court Ordered Disclosures Reveal a Pattern and Practice of Troubling FDIC Anti-Crypto Pressure on Banks

After more than a year of seeking these pause letters, with the FDIC opposing us each step of the way, the FDIC finally provided them in a form that reveals some of the underlying substance of those letters. The picture that they paint is one of a long-running, indiscriminate, and secretive campaign by the FDIC to prevent banks from using or offering a wide range of crypto products and services.

The letters¹⁵ speak for themselves:

- April 15, 2022: A bank is asked to "pause all crypto asset-related activity" related to a proposed product that would have offered "bank customers access to Bitcoin and Ethereum through the bank's mobile app." (Letter 6)
- May 4, 2022: A bank is asked "not [to] implement [a] product" that "would provide bank customers an avenue to engage in crypto asset transactions, specifically the purchase and sale of Bitcoin, using the bank's mobile banking application." (Letter 9)
- August 26, 2022: The FDIC requests that a bank "refrain from providing" a service to its customers that would have allowed "customers the ability to buy, hold, and sell bitcoin." (Letter 18)
- September 9, 2022: The FDIC asked that a bank "not proceed with planned activities" until the FDIC completed its review, after the bank informed the FDIC that it was "developing a Digital Asset department... to implement the following crypto-asset

¹² Appendix B, FDIC FOIA Litigation, Docket Entry 26-1.

¹³ FDIC FOIA Litigation, December 12, 2024 Minute Order.

¹⁴ *Id.*

¹⁵ Appendix C, FDIC FOIA Litigation, Docket Entry 27-2.

services for bank customers: custodian services...; facilitation of buying and selling crypto-assets...; and, allowing customers to spend/withdraw bitcoin.” (Letter 19)

- October 17, 2022: “[T]he Bank acquired three types of crypto-assets and subsequently exchanged less than \$25,000 in crypto-assets for Non-Fungible Tokens (NFT)....Until we complete our review, we request the Bank refrain from purchasing additional crypto-assets and NFTs.” (Letter 22)
- May 5, 2023: Upon receiving a bank’s notice of its intent to provide a bank account to a third party “for the purpose of holding deposit reserves corresponding to [the third party’s] issuance of a stablecoin”, the FDIC told the bank that it “should not proceed with any crypto-asset activity until” an unspecified time at the FDIC’s discretion. (Letter 25)

Beyond these examples, the FDIC sent more than a dozen additional letters similarly asking financial institutions to pause crypto-related projects with unspecified review periods. And one particularly sinister aspect of these letters is that they were often sent to senior leadership at financial institutions, such as the Board of Directors, not lower level employees who typically interact with regulators about day-to-day operations. We think this was intended to send a message to bank leadership and the entire industry: engage with crypto at your own peril.

These FDIC actions have been carried out away from public scrutiny, without input from industry players. This behind-the-scenes bias against crypto not only has undermined the principles of a transparent government but has also stymied the growth and potential of the digital economy. What’s more, while the FDIC was sending these pause letters, the FDIC and other banking regulators were publicly denying that they were discouraging banking organizations from providing banking services to customers for any type of lawful activity.¹⁶

Whether you are a crypto enthusiast or a skeptic, the lack of transparency in these regulatory actions and the contradictions between what was happening privately versus what the regulators were saying publicly should alarm everyone. It is essential for all parties to recognize this issue and address it head-on, especially when regulatory actions are justified under the guise of guarding against vague concerns of systemic risk without clear timelines for lifting pauses that left regulated entities in bureaucratic limbo.

The FDIC Still Has Not Remediated These Issues

The FDIC’s OIG Report initially highlighted these problems and made two specific recommendations for the FDIC to remediate these issues: (1) “establish a plan with timeframes for assessing risks pertaining to crypto-related activities”; and (2) “update and clarify the supervisory feedback process related to its review of supervised institutions’ crypto-related

¹⁶ Federal Reserve, FDIC, and OCC, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 3, 2023), available at <https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf> (“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.”); Federal Reserve, FDIC, and OCC, *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities* (Feb. 23, 2023), available at <https://bit.ly/3FJ7QbS> (same quote).

activities.”¹⁷ The FDIC agreed with both recommendations and proposed to complete all corrective actions by January 30, 2024.¹⁸

Despite it being more than a year since the FDIC stated that it would complete these corrective actions, the FDIC OIG’s website makes clear that this recommendation remains unimplemented as of today.¹⁹ And although the FDIC recently publicized an internal memorandum that purports to address this issue by instructing its regional offices to establish supervisory timeframes, the FDIC still has not *itself* established those timeframes (as the FDIC OIG recommended) and has provided only vague guidance to its regional offices on the issue.²⁰ This is the exact type of willful inaction and feet-dragging that forces crypto companies to languish in regulatory purgatory.

The FDIC’s internal memorandum also purports to address the FDIC OIG’s second recommendation. But that memorandum was made public only recently—and only because the agency released it reactively in response to a FOIA request.²¹ Prior to that, it was not at all clear to the public how the FDIC updated and clarified the supervisory feedback process related to its review of supervised institutions’ crypto-related activities. And even in the memo, the FDIC only half-heartedly addresses the FDIC OIG’s concerns in a few sentences. If the FDIC OIG felt this issue was important enough to issue its public report and propose corrective action, it should have been important enough for the FDIC to publicly explain—immediately and in detail—how it corrected its behavior, instead of leaving crypto companies and financial institutions in the dark.

Why This Matters

The FOIA litigation against the FDIC highlights four broader concerns about regulatory overreach and transparency:

1. **Lack of Transparency:** Regulators’ refusal to disclose information undermines public trust in their decision-making processes. The absence of transparency prevents meaningful oversight and accountability.
2. **Bias in Regulatory Actions:** The underlying anti-crypto pressure and reluctance to provide information suggest that regulatory actions may have been influenced by bias or hidden agendas rather than objective assessments of risks.
3. **Impact on the Crypto Industry:** The confidential nature of the FDIC’s ‘pause letters’ and other supervisory actions has created a chilling effect on banks and other financial institutions, making it more difficult for crypto companies to operate in the United States.

¹⁷ Appendix A, OIG Report, pp. ii-iii.

¹⁸ *Id.*

¹⁹ FDIC OIG List of Unimplemented Recommendations, as of February 4, 2025, <https://www.fdicogov/unimplemented-recommendations>

²⁰ <https://www.fdic.gov/foia/fdic-memorandum-procedures-reviewing-notifications-engagement-crypto-related-activities>

²¹ <https://www.fdic.gov/foia/foia-reading-room> (listing the internal memorandum among documents disclosed in response to FOIA requests)

4. **Broader Implications for Regulatory Accountability:** Coinbase's litigation serves as an example of how regulators can act unilaterally and in secret to marginalize a legal industry without being held accountable.

Outcome and Current Status

As of now, our FOIA litigation has forced the FDIC to release some documents, but the process remains ongoing. The released materials have provided glimpses into how the FDIC applied pressure on financial institutions behind closed doors, but significant questions remain unanswered due to continued stonewalling. And following a recent hearing, the Court agreed with Coinbase that the FDIC incorrectly interpreted our FOIA request narrowly and ordered the FDIC to search for and produce any additional pause letters that it has not already provided by the end of this week.²²

Coinbase's FOIA requests and subsequent litigation against the FDIC are not just about accessing documents—they're about holding regulators accountable for their actions. The outcome of this legal battle will have significant implications for the future of cryptocurrency in the U.S., as well as for the broader principles of transparency and fairness in regulatory practices.

A New Day

Despite these challenges, I remain optimistic about the future of cryptocurrency in America. We can turn the page and embrace a new day, one where innovation and consumer protection coexist. In order to achieve this goal, we need to facilitate access to banking services, which means starting with the banking agencies and the ability of banks to engage in crypto related activity. To that end, on February 3, 2025, Coinbase submitted a detailed letter to the OCC, the Federal Reserve Board, and the FDIC urging the agencies to eliminate barriers that prevent banks from offering cryptocurrency custody and execution services (C&E Services). We emphasized that these specified services can be safely provided on behalf of customers using new technologies and should be allowed to be outsourced to third-party providers like Coinbase under clear regulatory guidance and supervisory standards that are already in place.

Coinbase specifically requests the withdrawal of OCC Interpretive Letter 1179,²³ which imposes a de facto application process before new cryptocurrency banking activities may be undertaken or offered by any national bank. As used in practice, this letter conflicts with previous OCC Interpretive Letters 1170, 1172, and 1174, which describe the well-established legal basis supporting the permissibility of crypto-related activities for national banks. The withdrawal of IL 1179 would reaffirm national banks' authority to provide crypto custody services and facilitate

²² FDIC FOIA Litigation, January 22, 2025 Minute Order.

²³ *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, <http://occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf>

related transactions, thereby aligning with established legal precedents and promoting technological innovation in banking.

We argue state banks that are members of the Federal Reserve System, consistent with the Federal Reserve's Policy Statement,²⁴ should also be allowed to engage in the same cryptocurrency activities as national banks without additional constraints, provided these activities are authorized by state law. This is the stance the Federal Reserve ordinarily applies to ensure the equal treatment of national and state bank activities, regardless of the supervising agency, to help level the competitive playing field and mitigate risks of regulatory arbitrage. This principle supports state banks' rights to offer and outsource C&E Services in line with national banks' capabilities, and subject to appropriate third-party risk management practices being established.

Federal law similarly empowers state nonmember banks to engage in C&E Services and related outsourcing agreements if authorized by state law. Coinbase points out that the FDIC's current guidance, particularly FDIC Interpretive Letter 16-2022 ("FIL 16-2022")²⁵, has been applied in a manner inconsistent with its past practices for equivalent prior notice processes and effectively hinders these banks from participating in legally permissible cryptocurrency activities. By removing such restrictions, state nonmember banks would be better positioned to integrate cryptocurrency C&E Services into their customer offerings, benefiting from new technologies while adhering to established safety and soundness principles.

Coinbase's letter ultimately urges the banking agencies to support the withdrawal of IL 1179, reaffirm that existing laws and regulations permit banks to provide and outsource cryptocurrency C&E Services, and clarify banks' abilities to use new technologies through outsourcing relationships, subject to appropriate risk management standards being established. These actions would eliminate regulatory uncertainties for banks, foster collaboration between banks and third-party providers, and promote a robust, innovative financial system for crypto companies across the country. By aligning with existing legal frameworks and President Trump's January 23rd Executive Order on Digital Financial Technology, the agencies can ensure that the U.S. remains a leader in financial innovation.

Conclusion

The lack of transparency, the extensive coercive tactics, and the egregious abuse of regulatory processes not only harm the crypto industry but also erode public trust in our institutions. America has always been a leader in innovation, and we must not allow these efforts to stifle our progress. This committee should be commended for exploring both the harms done by the banking regulators, and the need for reform. We suggested a few actions the regulators could

²⁴ FRB Policy Statement on Section 9(13) of the FRA, 88 Fed. Reg. 7848 (Feb. 7, 2023) ("Policy Statement"); 12 C.F.R. § 208.112.

²⁵ FDIC Interpretive Letter 16-2022, *Notification of Engaging in Crypto-Related Activities*, April 7, 2022. <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>

take to reverse the harmful effects of debanking, but we also urge this committee to consider additional measures that would improve transparency and public input within the agencies.

Thank you to both sides of the aisle for your continued commitment to ensuring the United States remains at the forefront of financial and technological innovation, and I look forward to your questions.

Appendix A



FDIC Strategies Related to Crypto-Asset Risks

October 2023

EVAL-24-01

Evaluation Report Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

**REDACTED VERSION
PUBLICLY AVAILABLE**

The redactions contained in this report are based upon requests from FDIC senior management to protect the Agency's information from disclosure.



NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.



Executive Summary

FDIC Strategies Related to Crypto-Asset Risks

According to a September 2022 White House Fact Sheet, millions of people globally, including 16 percent of adult Americans, have purchased crypto assets. The Fact Sheet also stated, crypto assets “present potential opportunities to reinforce the U.S. leadership in the global financial system and remain at the technological frontier.” Executive Order 14067 (March 2022) stated that the U.S. has an interest in responsible financial innovation and expanding access to safe and affordable financial services using crypto assets. The Executive Order also stated that the U.S. has an interest in reducing the cost of domestic and cross-border funds transfers and payments and modernizing its public payment systems, which may be possible through the use of crypto assets.

While crypto assets present many potential opportunities and benefits, they also pose a number of risks to the U.S. financial system. In recent years, the crypto-asset sector has experienced significant volatility. The total market capitalization of crypto assets fluctuated from about \$132 billion in January 2019 to \$3 trillion in November 2021. More concerning, the market capitalization has fallen by 60 percent to \$1.2 trillion as of April 2023. These events highlight various risks that the crypto-asset sector could pose to financial institutions, including liquidity, market, pricing, and consumer protection risks. Financial institutions can be exposed to crypto-asset risks when providing services to crypto-asset companies or engaging in crypto-asset-related activities.

While currently limited, if material exposure of financial institutions to the risks posed by crypto-related activities were to manifest, it may affect the Federal Deposit Insurance Corporation’s (FDIC) mission to maintain stability and public confidence in the Nation’s financial system. The FDIC carries out its mission by, among other things, supervising and examining financial institutions for safety and soundness and consumer protection. The exposure of financial institutions to the risks posed by crypto-related activities presents safety and soundness risks and consumer protection concerns. According to the FDIC, it is taking a deliberate and cautious approach to bank participation in crypto-related activities.

As stated in Executive Order 14067, crypto assets present numerous opportunities to foster innovation and cost savings. The FDIC has an opportunity to take actions to uphold the United States’ interests in the financial sector. However, because crypto assets also pose significant risks to the financial sector, the FDIC should ensure it

Executive Summary

can effectively address those risks, and promote safety and soundness and consumer protection.

The objective of our review was to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets.

Results

The FDIC has started to develop and implement strategies that address the risks posed by crypto assets. However, the Agency has not assessed the significance and potential impact of the risks. Specifically, the FDIC has not yet completed a risk assessment to determine whether the Agency can sufficiently address crypto-asset-related risks through actions such as issuing guidance to supervised institutions. In addition, the FDIC's process for providing supervisory feedback on FDIC-supervised institutions' crypto-related activities is unclear. As part of its process, the FDIC requested financial institutions to provide information pertaining to their crypto-related activities. Additionally, the FDIC issued letters (pause letters), between March 2022 and May 2023, to certain FDIC-supervised financial institutions asking them to pause, or not expand, planned or ongoing crypto-related activities, and provide additional information. However, the FDIC did not (1) establish an expected timeframe for reviewing information and responding to the supervised institutions that received pause letters, and (2) describe what constitutes the end of the review process for supervised institutions that received a pause letter.

Until the FDIC assesses the risks of crypto activities and provides supervised institutions with effective guidance, the FDIC and some FDIC-supervised institutions may not take appropriate actions to address the most significant risks posed by crypto assets. In addition, based on evidence obtained during our evaluation, the FDIC's lack of clear procedures causes uncertainty for supervised institutions in determining the appropriate actions to take. If financial institutions do not receive timely feedback from the FDIC and do not understand what constitutes the end of the FDIC's review process, this uncertainty creates risk that the FDIC will be viewed as not being supportive of financial institutions engaging in crypto-related activities.

Recommendations

This report contains two recommendations for the FDIC to: (1) establish a plan with timeframes for assessing risks pertaining to crypto-related activities and (2) update

Executive Summary

and clarify the supervisory feedback process related to its review of supervised institutions' crypto-related activities.

The FDIC concurred with both report recommendations and proposed corrective actions that were sufficient to address the intent of the recommendations. Therefore, we consider these recommendations to be resolved and open pending completion of the corrective actions. The FDIC plans to complete all corrective actions by January 30, 2024.

Contents

BACKGROUND.....	3
EVALUATION RESULTS	8
The FDIC Should Continue Its Efforts to Assess Risks Related to Crypto Assets	8
The FDIC Should Improve Its Supervisory Feedback Process for Crypto-Related Activities	11
FDIC COMMENTS AND OIG EVALUATION.....	13

Appendices

1. Objective, Scope, Methodology	15
2. Acronyms and Abbreviations	17
3. FDIC Comments	18
4. Summary of the FDIC's Corrective Actions	23

Figure

1. Crypto-Asset Market Capitalization – January 2019 to April 2023	2
--	---



Federal Deposit Insurance Corporation
Office of Inspector General
Audits, Evaluations, and Cyber

October 17, 2023

Subject | FDIC Strategies Related to Crypto-Asset Risks

According to a September 2022 White House Fact Sheet, millions of people globally, including 16 percent of adult Americans, have purchased crypto assets.¹ The Fact Sheet also stated, crypto assets “present potential opportunities to reinforce the U.S. leadership in the global financial system and remain at the technological frontier.” A March 2022 Executive Order stated that the U.S. has an interest in responsible financial innovation and expanding access to safe and affordable financial services using crypto assets.² The Executive Order also stated that the U.S. has an interest in reducing the cost of domestic and cross-border funds transfers and payments and modernizing its public payment systems that may be possible through the use of crypto assets.³

In March 2022, the U.S. Government Accountability Office (GAO) issued a report that described a number of benefits resulting from crypto assets.⁴ According to GAO, cryptocurrencies, a type of crypto asset, are growing as a means of payment by individuals, businesses, and governments around the world. Because cryptocurrencies are digitally based and generally do not depend on intermediaries, they have the potential to reduce user costs. In addition, cryptocurrency users can conduct transactions in a manner that may provide greater privacy for their financial activities.

While crypto assets present many potential opportunities and benefits, they also pose a number of risks to the U.S. financial system. In recent years, the crypto-asset sector has experienced significant volatility. As shown in Figure 1, the total market capitalization of crypto assets fluctuated from about \$132 billion in January 2019 to \$3 trillion in November 2021. More concerning, the market capitalization has fallen by 60 percent to \$1.2 trillion as of April 2023. These events highlight various risks

¹ *FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets* (September 16, 2022). By “crypto asset,” the FDIC refers generally to any digital asset implemented using cryptographic techniques.

² Executive Order 14067, *Ensuring Responsible Development of Digital Assets* (March 9, 2022). The FDIC has determined that Executive Order 14067 is non-binding on the FDIC. We have included discussion of the Executive Order in this report because it provides context to the Federal Government’s overall approach to crypto assets.

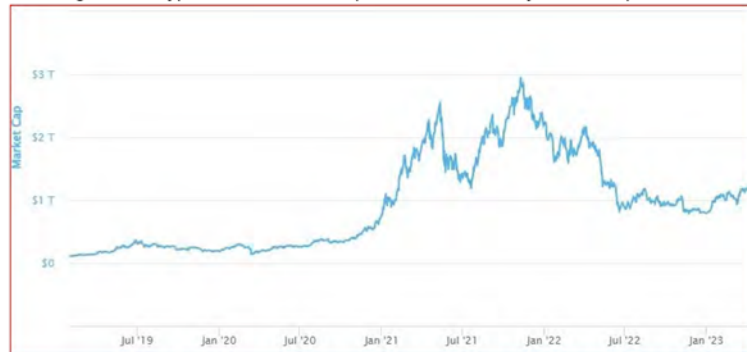
³ Public payment systems are mechanisms established to facilitate the clearing and settlement of monetary and other financial transactions.

⁴ Government Accountability Office, *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges*, GAO-22-104625 (March 2022).

FDIC Strategies Related to Crypto-Asset Risks

that the crypto-asset sector could pose to financial institutions, including liquidity, market, pricing, and consumer protection risks.⁵ Financial institutions can be exposed to crypto-asset risks by providing services to crypto-asset companies or by engaging in crypto-related activities.⁶

Figure 1: Crypto-Asset Market Capitalization—January 2019 to April 2023



Source: CoinMarketCap data as of July 26, 2023

While currently limited, if material exposure of financial institutions to the risks posed by crypto-related activities were to manifest, it may affect the Federal Deposit Insurance Corporation's (FDIC) mission to maintain stability and public confidence in the Nation's financial system. The FDIC carries out its mission by, among other things, supervising and examining financial institutions for safety and soundness and consumer protection. The exposure of financial institutions to the risks posed by crypto-related activities presents safety and soundness risks and consumer protection concerns. According to the FDIC, the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC), financial institutions should be aware of a number of key risks. These risks include:

- Volatility in crypto-asset markets which could potentially impact deposit flows associated with crypto-asset companies.

⁵ For purposes of this report, a financial institution means either 1) a state-chartered bank or savings institution that is not a member of the Federal Reserve System or 2) an FDIC-insured depository institution. We use the terms "bank" and "financial institution" interchangeably throughout this report.

⁶ In FIL-16-2022, the FDIC defined the term "crypto-related activities" to include 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. The FIL stated 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.

FDIC Strategies Related to Crypto-Asset Risks

- Susceptibility to stablecoin run risk which could potentially impact deposit outflows for banking organizations that hold stablecoin reserves.⁷
- Contagion risk resulting from interconnections among certain crypto-asset participants, including through lending, investing, funding, service, and operational arrangements. These interconnections may also lead to concentration risks for financial institutions with exposures to the crypto-asset sector.

As stated in Executive Order 14067, crypto assets present numerous opportunities to foster innovation and cost savings. The FDIC has an opportunity to take actions to uphold the United States' interests in the financial sector. However, because crypto assets also pose significant risks to the financial sector, the FDIC should ensure it can effectively address those risks, and promote safety and soundness and consumer protection.

The objective of our review was to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation*. Appendix 1 presents our evaluation objective, scope, and methodology.

BACKGROUND

The FDIC achieves its mission, in part, by carrying out a supervision program to promote safe and sound operations at financial institutions and ensure compliance with federal consumer protection laws. Further, the FDIC is responsible for managing resolutions and receiverships. The Division of Risk Management Supervision (RMS) supervises financial institutions to help ensure that they operate in a safe and sound manner; the Division of Depositor and Consumer Protection (DCP) supervises financial institutions to promote compliance with federal consumer protection laws and regulations; and the Divisions of Resolutions and Receiverships (DRR) and Complex Institution Supervision and Resolution close and liquidate failing and failed institutions.

FDIC Efforts to Address Crypto-Asset Risks

The FDIC developed an initial approach to address crypto-asset risks in 2021. The FDIC's approach, at that time, included a plan to provide clear guidance to the public on: (1) how the FDIC's existing rules and policies apply to crypto assets, (2) the

⁷ The term "stablecoins" refers to a category of cryptocurrencies with mechanisms that are aimed at maintaining a stable value, such as by tying the value of the coin to a specific currency, asset, or pool of assets or by algorithmically controlling supply in response to changes in demand in order to stabilize value.

FDIC Strategies Related to Crypto-Asset Risks

types of activities that are permissible for financial institutions to engage in, and (3) the FDIC's supervisory expectations for financial institutions that engage in such activities. The approach also included working with the FRB and OCC to coordinate policies for how and under what circumstances financial institutions can engage in activities involving crypto assets.

In 2022, the FDIC shifted to a "bottom up" approach to understanding crypto-asset risks. In March 2022, the FDIC established the Crypto Asset Risks Interdivisional Working Group to focus on this new (and still current) approach to crypto-asset risks.⁸ According to the FDIC, its current approach to engaging with supervised institutions as they consider crypto-related activities includes: (1) developing an understanding of supervised institutions' crypto-related activities, (2) providing institutions with case-specific supervisory feedback, and (3) providing broader industry guidance on an interagency basis.

To gain an understanding of the crypto-related activities and the associated risks, on April 7, 2022, the FDIC issued Financial Institution Letter (FIL) 16-2022, *Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities*. The FIL requested that FDIC-supervised institutions notify the FDIC if they intended to engage in, or were currently engaged in, crypto-related activities. The FIL requested that institutions "provide information necessary to allow the agency to assess the safety and soundness, consumer protection, and financial stability implications of such activities." Also, the FIL stated that the FDIC will review the notification and information received and request additional information as needed. In addition, the FIL stated that the FDIC would provide relevant supervisory feedback to the FDIC-supervised institution, as appropriate, in a timely manner. The FRB and OCC have issued similar requests to their supervised institutions.⁹

In response to FIL 16-2022, a number of FDIC-supervised institutions provided notifications of their intent to engage in, or engagement in, crypto-related activities. According to FDIC data, as of January 2023, the Agency was aware of 96 FDIC-supervised financial institutions that either had expressed interest or were engaged in crypto-related activities. Some of these activities included crypto-asset-custody services, deposit services, crypto-asset-collateralized lending, and facilitation of customer purchase and sale of crypto assets through a third party.

In June 2022, the Directors of RMS and DCP issued a memorandum to the Regional Directors (RD memo) to facilitate the tracking and review of notifications received in

⁸ The FDIC's Crypto Asset Working Group includes: RMS, DCP, DRR, Division of Insurance and Research, Division of Complex Institution Supervision and Resolution, and the Legal Division.

⁹ Federal Reserve SR 22-6 / CA 22-6: *Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations* (August 16, 2022); OCC, Interpretive Letter 1179 (November 18, 2021).

FDIC Strategies Related to Crypto-Asset Risks

response to the FIL.¹⁰

(b) (8)

[REDACTED]

RD memo in October 2022

(b) (8)

The FDIC amended the

[REDACTED]

According to the FDIC, as part of its review of financial institutions' crypto-related activities, between March 2022 and May 2023, the FDIC sent letters to [REDACTED] supervised institutions. The letters asked that the institutions pause from proceeding with planned activities or expanding existing activities and to provide additional information. The FDIC asked these [REDACTED] financial institutions to pause their crypto-related activities in order to assess the safety and soundness, consumer protection, and financial stability implications of such activities before providing supervisory feedback. According to the FDIC, as of August 2023, the FDIC had provided [REDACTED] of these [REDACTED] supervised institutions with supervisory feedback related to their planned or ongoing crypto-related activities.¹¹

FDIC Efforts to Address Crypto-Related Activities of Failed Institutions

The resolution of failing or failed institutions (FFI) engaged in crypto-related activities poses complex challenges to the FDIC. The challenges include the assessment of franchise value, operational considerations, and deposit insurance determinations. As a result, DRR developed a strategy to address these challenges. In January 2021, DRR began developing a Digital Assets Operational Plan to ensure its readiness to respond to and execute on resolution scenarios related to crypto assets.

¹⁰ Regional Director Memorandum, *Procedures for Reviewing Notifications of Engagement in Crypto-Related Activities* (June 6, 2022, amended October 31, 2022).

¹¹ According to the FDIC, the Agency has provided [REDACTED] supervised institutions with supervisory feedback related to their planned or ongoing crypto-related activities. Only [REDACTED] of these [REDACTED] institutions had received a pause letter.

FDIC Strategies Related to Crypto-Asset Risks

In December 2022, DRR completed the first phase of its plan by developing and documenting five known potential use cases.¹² According to DRR, this plan will be a living document, and DRR will update the plan as new digital asset activities, legislative developments, and advances in technology emerge. In addition, DRR entered into a contract for crypto-asset management and liquidation services associated with FFIs.

FDIC Efforts to Address Misrepresentations of Deposit Insurance

A separate, but related issue, is the risk of misrepresentations about FDIC deposit insurance by non-bank entities (such as crypto companies). In 2022, a cryptocurrency company filed for bankruptcy. This company had been misrepresenting to its customers for over a year that the funds it held for customers were insured by the FDIC. In July 2022, the FDIC and FRB issued a joint letter demanding that this firm cease and desist from making such claims. According to the FDIC, between July 2022 and June 2023, the Agency issued 11 additional public advisory letters to non-bank entities that appeared to be making crypto-related misrepresentations about FDIC deposit insurance.¹³ These advisory letters demanded that the recipients stop making false and misleading statements regarding FDIC deposit insurance and take immediate action to address these misleading and false statements or to provide documentation that their claims are true and accurate.¹⁴ The FDIC also issued *FIL 35-2022 Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies*, and a *Fact Sheet: What the Public Needs to Know About FDIC Deposit Insurance and Crypto Companies*. *FIL 35-2022* and the Fact Sheet provided additional information about deposit insurance coverage and the risks of misrepresentations of FDIC insurance coverage.

The FDIC obtains information on potential deposit insurance misrepresentations through various methods, including monitoring three public portals. DCP monitors two of the portals, which also contain other consumer protection and deposit insurance complaints. The Legal Division created the third portal in July 2022.¹⁵ This third portal is focused on complaints and inquiries related to misrepresentations of deposit insurance. Along with setting up the new portal, the FDIC updated internal

¹² The five potential use cases include: (1) crypto assets held and owned by the FFI, (2) crypto assets held by the FFI as loan collateral, (3) crypto assets held by the FFI in custody for customers, (4) bank-created stabletoken on a permissioned ledger, and (5) a multibank permissioned payment system.

¹³ These 11 letters do not represent all public advisory letters that the FDIC has issued regarding misrepresentations about FDIC deposit insurance. For purposes of this report, we included the number of letters issued to address crypto-related misrepresentations only.

¹⁴ The Federal Deposit Insurance Act prohibits any person from representing or implying that an uninsured deposit is insured or from knowingly misrepresenting the extent and manner in which a deposit liability, obligation, certificate, or share is insured and authorizes the FDIC to enforce these prohibitions. 12 U.S.C. 1828(a)(4).

¹⁵ This portal was created as part of the FDIC's final rule on False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo, which became effective July 5, 2022. This rule established the process by which the FDIC will identify and investigate conduct that may violate section 18(a)(4) of the FDI Act.

FDIC Strategies Related to Crypto-Asset Risks

processes for evaluating, escalating, and responding to misrepresentation complaints and inquiries. The Legal Division is the primary group responsible for responding to misrepresentation issues.

Joint Statements by the Federal Regulatory Agencies

The FDIC, FRB, and OCC jointly issued a number of public statements regarding the risks posed by crypto assets in 2021 and 2023. In November 2021, the FDIC, FRB, and OCC issued a joint statement summarizing their interagency crypto-asset policy sprint initiative. The initiative set forth the agencies' plan to clarify the rules and regulations around how financial institutions can engage in crypto-related activities.¹⁶ In the joint statement, the agencies said that they planned to "provide greater clarity on whether certain activities related to crypto assets conducted by banking organizations are legally permissible." The agencies also stated that they planned to provide "expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations" related to certain crypto-related activities.¹⁷

In January and February 2023, the FDIC, FRB, and OCC issued two additional joint statements regarding financial institutions' crypto-related activities.¹⁸ In the January 2023 joint statement, the agencies highlighted key crypto-asset risks for financial institutions' awareness. The joint statement also outlined the agencies' views regarding whether certain crypto-related activities are consistent with safe and sound banking practices. The agencies stated 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."¹⁹ Further, the agencies warned that they 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." In the February 2023 joint statement, the agencies discussed the heightened liquidity risks presented by certain funding sources of crypto-asset-sector participants and offered methods to manage such risks. The February 2023 statement also discussed the importance of establishing and maintaining effective risk management and controls commensurate with the level of liquidity risks and provided examples of certain practices.²⁰

¹⁶ *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps* (November 2021).

¹⁷ The joint statement listed these crypto-related activities: (1) Crypto-asset safekeeping and traditional custody services, (2) Ancillary custody services, (3) Facilitation of customer purchases and sales of crypto assets, (4) Loans collateralized by crypto assets, (5) Issuance and distribution of stablecoins, and (6) Activities involving the holding of crypto assets on the balance sheet.

¹⁸ *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 2023).

¹⁹ Decentralized network generally refers to crypto-asset protocols and platforms that allow for some form of automated peer-to-peer transactions.

²⁰ *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities* (February 2023).

EVALUATION RESULTS

We found that the FDIC has started to develop and implement strategies that address the risks posed by crypto assets. For example, the FDIC identified the risks associated with its supervised financial institutions' crypto-related activities and issued FIL-16-2022, which established a strategy to review information financial institutions submitted pertaining to their crypto-related activities and provide supervisory feedback on these activities. However, the Agency has not assessed the significance and potential impact of the risks. Specifically, the FDIC has not yet completed a risk assessment to determine whether the Agency can sufficiently address crypto-asset-related risks through actions such as issuing guidance to supervised institutions. In addition, the FDIC's process for providing supervisory feedback under FIL-16-2022 is unclear. As part of its process, the FDIC issued letters (pause letters) to certain FDIC-supervised financial institutions asking them to pause, or not expand, planned or ongoing crypto-related activities. However, the FDIC did not (1) establish an expected timeframe for reviewing information and responding to the supervised institutions that received pause letters and (2) describe what constitutes the end of the review process for supervised institutions that received a pause letter.

Until the FDIC assesses the risks of crypto activities and provides supervised institutions with effective guidance, the FDIC and some FDIC-supervised institutions may not take appropriate actions to address the most significant risks posed by crypto assets. In addition, based on evidence obtained during our evaluation, the FDIC's lack of clear procedures causes uncertainty for supervised institutions in determining the appropriate actions to take. If financial institutions do not receive timely feedback from the FDIC and do not understand what constitutes the end of the FDIC's review process for paused crypto-related activities, this uncertainty creates risk that the FDIC will be viewed as not being supportive of financial institutions engaging in crypto-related activities.

The FDIC Should Continue Its Efforts to Assess Risks Related to Crypto Assets

The FDIC has identified numerous risks associated with its supervised financial institutions' crypto-related activities. However, the Agency has not yet assessed the significance and potential impact of these risks through a risk assessment. A risk assessment would enable the FDIC to determine whether the crypto-asset-related risks can be sufficiently addressed as identified in the Crypto Asset Risks Interdivisional Working Group ("Crypto Asset Working Group") Charter.

FDIC Strategies Related to Crypto-Asset Risks

The Crypto Asset Working Group Charter (May 2022) describes its mission as being “responsible for assessing the safety and soundness, consumer protection, deposit insurance, resolution planning, and financial stability risks associated with crypto-asset-related activities that are, or may be, engaged in by financial institutions.” The Charter further states that the group “shall report out its assessment of these risks, including whether such risks can be sufficiently mitigated, and, as appropriate, provide recommendations for addressing those risks to the relevant officers of the agency.”

The FDIC started to identify risks associated with financial institution crypto-related activities in its draft *Framework for Developing an FDIC Policy View on Digital Assets Potential [Insured Depository Institution] Activity, Assessment Approach, and Potential Policy Issues* (2021 Framework) and the draft *Facilitation Bottom-Up Risk Assessment Framework* (2022 Facilitation Framework) (September 26, 2022). In its 2021 Framework, the FDIC identified potential financial institution crypto-related activities and the Agency’s approach for analyzing risks and developing a policy view. The FDIC used this as a briefing document during a discussion on a 2021 FDIC Digital Assets Performance Goal with the former Chairman. In the 2022 Facilitation Framework, the FDIC identified numerous risks, including consumer protection risks and financial stability risks specifically associated with financial institutions’ crypto-asset-facilitation activities.²¹ The FDIC issued joint statements in January and February 2023, along with the FRB and OCC, which identified key crypto-asset risks and heightened liquidity risks presented by certain funding sources of crypto-asset-sector participants. However, the Crypto Asset Working Group has not completed a risk assessment of any of the crypto-related activities, including facilitation activities.

According to the GAO’s *Standards for Internal Control in the Federal Government* (September 2014) (Green Book), “Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.” It also states, “Management analyzes the identified risks to estimate their significance...”²² Furthermore, “Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance.”²³ The Green Book also states that documentation “provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a

²¹ Crypto-asset-facilitation activities are activities whereby a financial institution connects customers and third parties to facilitate the customers’ purchase and sale (trades) of crypto assets.

²² Green Book 7.06 states Management estimates the significance of the identified risks to assess their effect on achieving the defined objectives at both the entity and transaction levels. Management estimates the significance of a risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk. Magnitude of impact refers to the likely magnitude of deficiency that could result from the risk and is affected by factors such as the size, pace, and duration of the risk’s impact. Likelihood of occurrence refers to the level of possibility that a risk will occur. The nature of the risk involves factors such as the degree of subjectivity involved with the risk and whether the risk arises from fraud or from complex or unusual transactions.

²³ Green Book 6.08 defines risk tolerance as “the acceptable level of variation in performance relative to the achievement of objectives.”

FDIC Strategies Related to Crypto-Asset Risks

few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.”

According to the FDIC, it is taking a deliberate and cautious approach to bank participation in crypto-asset-related activities. However, the FDIC has not yet analyzed the crypto-asset risks and documented its assessment of them. Specifically, the FDIC has not assessed their significance in order to determine the magnitude of impact, likelihood of occurrence, and nature of the risks. Also, the FDIC has not developed mitigation strategies, such as issuing guidance to financial institutions, to ensure that risks are within the defined risk tolerance.

This occurred because the FDIC’s process for assessing and responding to risks related to FDIC-supervised institutions’ crypto-related activities is not mature. In early 2022, the FDIC adopted a new bottom-up approach to develop an understanding of supervised institutions’ crypto-asset-related activities and the associated risks. Since that time, the FDIC has made efforts to address crypto-asset risks, such as issuing two FILs, the RD memo, two interagency joint statements, and a number of public advisory letters to crypto-asset companies. While these efforts are positive and necessary to understanding the risks posed by crypto assets, the FDIC must continue its work to fully understand and address the risks.

If the FDIC does not assess the significance of the risks posed by crypto assets, it might not take appropriate actions to address them. The FDIC should conduct risk assessments as a basis to develop mitigation strategies. Without a risk assessment, the FDIC may not develop and issue effective policies, procedures, and guidance to address these risks.

If the FDIC does not provide its supervised institutions with effective guidance, the FDIC and some FDIC-supervised institutions may not take appropriate actions to address the most significant risks posed by crypto assets. This could impact the FDIC’s mission to promote financial stability. The FDIC promotes financial stability, in part, by ensuring safe and sound financial institution practices and protecting consumers from financial harm. Absent effective guidance, financial institutions may not employ safe and sound practices to mitigate risks while developing innovative strategies and business lines to stay competitive in the financial marketplace.

Recommendation

We recommend that the Crypto Asset Risks Interdivisional Working Group:

1. Establish a plan with timeframes for assessing risks pertaining to crypto-related activities by:
 - a) Continuing to identify and document crypto-asset risks,

FDIC Strategies Related to Crypto-Asset Risks

- b) Performing and documenting an analysis of the identified risks to estimate their significance, and
- c) Developing and documenting strategies to address crypto-asset risks.

The FDIC Should Improve Its Supervisory Feedback Process for Crypto-Related Activities

The FDIC issued FIL-16-2022 which established a strategy to review information financial institutions submitted pertaining to their crypto-related activities and provide supervisory feedback on these activities. However, the FDIC's process for providing supervisory feedback to FDIC-supervised institutions about their crypto-related activities is unclear. The FDIC asked some financial institutions to pause or refrain from expanding certain crypto-related activities until it completed a review and provided supervisory feedback. Under the FIL, the FDIC was to provide timely, relevant, supervisory feedback. However, the FDIC did not establish an expected timeframe for reviewing the activities and responding to the FDIC-supervised institutions that received a pause letter. Also, the FDIC did not define what constitutes the end of its review process for institutions that received a pause letter. While the FDIC has maintained communication with these institutions, the lack of a clear end to the review process results in an extended pause and uncertainty for some institutions.

According to the FDIC, between March 2022 and May 2023, the FDIC sent letters to [REDACTED] supervised institutions as part of its review of the institutions' crypto-related activities. The letters (pause letters) asked that the institutions pause from proceeding with planned activities or expanding existing activities and provide additional information. The pause letters stated that the institutions should provide additional information "in advance of implementation," "pause all crypto asset-related activities," or "not proceed with any crypto-asset activity." The FDIC asked the institutions to pause their activities in order to review the institutions' crypto-related activities before providing supervisory feedback. The activities that institutions provided information on include crypto-asset-custody services, facilitation of customer purchase and sale of crypto assets through a third party, and crypto-asset-collateralized lending. According to the FDIC, as of August 2023, out of the [REDACTED] supervised institutions that received a pause letter, the FDIC had only provided [REDACTED] institutions with supervisory feedback. (b) (8) supervised institutions have decided not to pursue crypto-related activities or are no longer FDIC-supervised.²⁴ The remaining [REDACTED] have not received any supervisory feedback from the FDIC.

²⁴ There are (b) (8) additional supervised institutions that are no longer pursuing crypto activities or are no longer FDIC-supervised, but these (b) (8) institutions are included within the [REDACTED] institutions that received supervisory feedback.

FDIC Strategies Related to Crypto-Asset Risks

Review Timeframe Not Established

The FDIC did not establish an expected timeframe for reviewing the institutions' activities and responding to the FDIC-supervised institutions that received pause letters. According to FIL 16-2022, "[t]he FDIC will provide relevant supervisory feedback to the FDIC-supervised institution, as appropriate, **in a timely manner**" (emphasis added). The FDIC established procedures for reviewing and responding to notifications under the FIL in an RD memo. The RD memo, however, (b) (8)

(b) (8) The FDIC pause letters also did not provide the financial institutions with a timeframe for FDIC review of the information nor a timeframe for providing supervisory feedback.

Review End Process Not Described

FDIC procedures do not describe what constitutes the end of the review process for supervised institutions that received a pause letter. The RD memo states that (b) (8)

(b) (8) (b) (8) It also states that (b) (8) (b) (8) An FDIC official described final supervisory feedback as "the final version of the supervisory feedback to be transmitted to the bank." This official further stated the term "does not have a special meaning beyond being the last stage of the internal review process." The FDIC's procedures do not describe the end of the review process and what the final supervisory feedback entails. By not clearly stating or documenting what constitutes the end of the FDIC's review process, the FDIC may be causing confusion for the financial institutions that received a pause letter. For example, when one institution provided information on its planned crypto-related activities to the FDIC, it requested that the FDIC provide its approval of those activities. However, in the pause letter sent to the supervised institution, the FDIC stated that the FIL "does not provide for the issuance of an FDIC non-objection...."²⁵ The letter requested that the institution "not proceed with planned activities, pending FDIC supervisory feedback." This example demonstrates that the institution may be confused about what would constitute the end of the FDIC's review process.

According to the GAO *Standards for Internal Control in the Federal Government*, "[m]anagement documents in policies... its responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness." Policies may be further defined through day-to-day procedures. These procedures may "include the timing of when a control activity

²⁵ A non-objection is when the banking regulatory agency communicates to the institution that it does not object to the activity.

FDIC Strategies Related to Crypto-Asset Risks

occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified.”

The RD memo did not include an expected timeframe for reviewing a financial institution’s information and responding to an institution that received a pause letter. It also did not describe the end of the review process for these institutions. This occurred because the FDIC’s process for reviewing and responding to information received from FDIC-supervised institutions’ crypto-related activities is not mature. In early 2022, the FDIC adopted a new bottom-up approach to understand crypto-asset risks through use cases. The FDIC is continuing this effort in 2023.

Based on evidence obtained during our evaluation, including our independent evaluation of the FDIC’s process, discussions with FDIC personnel, and statements made by individuals in the banking and crypto-asset industries, we determined that the FDIC’s lack of clear procedures and timely feedback regarding crypto-asset activities causes uncertainty for supervised institutions in determining the appropriate actions to take. While the FDIC has maintained communication with these institutions, the lack of a clear end to the review process results in an extended pause and uncertainty for some institutions. The uncertainty in the process creates risk that the FDIC will be viewed as not being supportive of financial institutions participating in crypto activities. Such a view leads to risk that the FDIC would inadvertently limit financial institution innovation and growth in the crypto space. This view has also been expressed by individuals in the banking and crypto-asset industries alleging that financial regulators have been cutting off crypto firms from accessing the banking system and stifling innovation.

Recommendation

We recommend that the Director of the Division of Risk Management Supervision:

2. Update and clarify the supervisory feedback process to (a) establish an expected timeframe for reviewing information and responding to FDIC-supervised institutions pursuant to the Financial Institution Letter and (b) describe what constitutes the completion of its review of its supervised institutions’ crypto-related activities.

FDIC COMMENTS AND OIG EVALUATION

The FDIC’s Director of RMS provided a written response, dated September 27, 2023, to a draft of this report. The response is presented in its entirety in Appendix 3.

FDIC Strategies Related to Crypto-Asset Risks

In its response, the FDIC concurred with both report recommendations. The FDIC's proposed corrective actions were sufficient to address the intent of both recommendations, and the FDIC plans to complete corrective actions for these recommendations by January 30, 2024. We consider both recommendations to be resolved.

Both recommendations in this report will remain open until we confirm that corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 4.

Objective

The evaluation objective was to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets.

We conducted this evaluation from June 2022 through June 2023 in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation* (issued December 2020).

Scope and Methodology

The scope of our evaluation focused on the FDIC's efforts to develop and implement strategies that address crypto-asset risks. To obtain an understanding of the FDIC's efforts, we interviewed FDIC officials and staff from the Crypto Asset Risks Interdivisional Working Group, the Division of Risk Management Supervision, the Division of Depositor and Consumer Protection, the Division of Resolutions and Receiverships, the Division of Complex Institution Supervision and Resolution, and the Legal Division. Additionally, we reviewed the following relevant FDIC documents:

- Digital Assets Operational Plan (Revised December 2022);
- Division of Resolutions and Receiverships contract with a third party for crypto-asset services to support resolution and receivership activities (effective September 2021);
- *Draft Framework for Developing an FDIC Policy View on Digital Assets Potential [Insured Depository Institution] Activity, Assessment Approach, and Potential Policy Issues* (2021);
- *Draft Facilitation Bottom-Up Risk Assessment Framework* (September 26, 2022);
- FDIC public advisory letters issued to companies that appeared to be making crypto-related false or misleading representations about FDIC deposit insurance (Letters issued between July 2022 and June 2023);
- FDIC letters issued to certain FDIC-supervised institutions asking for additional information on planned or ongoing crypto-related activities, and pause from proceeding with planned activities or expanding existing activities (Letters issued between March 2022 and May 2023);
- FDIC's Crypto-Related Activity Tracking System data (as of January 2023);
- Financial Institution Letter 16-2022, *Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities* (April 7, 2022);
- Financial Institution Letter 35-2022 *Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies*, and *Fact*

Objective, Scope, and Methodology

Sheet: What the Public Needs to Know About FDIC Deposit Insurance and Crypto Companies (July 29, 2022);

- Regional Director Memorandum, *Procedures for Reviewing Notifications of Engagement in Crypto-Related Activities* (June 6, 2022, amended October 31, 2022);
- *Remarks by FDIC Chairman Jelena McWilliams at Money 20/20* (October 2021);
- *Remarks by FDIC Acting Chairman Martin J. Gruenberg at the Brookings Institution on The Prudential Regulation of Crypto-Assets* (October 2022);
- The Crypto Asset Risks Interdivisional Working Group Charter (May 2022); and
- The Crypto Asset Risks Interdivisional Working Group minutes (April 2022 through February 2023).

We also reviewed joint statements issued by the FDIC, OCC, and FRB: *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps* (November 23, 2021); *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 3, 2023); and *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities* (February 23, 2023).

We further reviewed Executive Order No. 14067, *Executive Order on Ensuring Responsible Development of Digital Assets* (March 9, 2022) and the associated reports directed by the Executive Order. Moreover, we reviewed the GAO Report, *Emerging Technology Offers Benefits for Some Applications but Faces Challenges*, GAO-22-104625 (March 2022).

To gain an understanding of the FDIC's supervisory actions provided to its supervised institutions regarding their crypto-related activities, we selected a sample of nine institutions engaged in or planning to engage in crypto-related activities. We selected the sample from the FDIC's Crypto-Related Activity Tracking System (as of October 2022). For this sample, we reviewed the FDIC's examination or visitation documentation, correspondence, and letters issued as of January 2023.

In addition, we reviewed FRB's SR 22-6 / CA 22-6: *Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations* (August 16, 2022) and the OCC Interpretive Letter 1179 (November 18, 2021). We further interviewed these two Federal banking regulatory agencies to obtain information on their efforts in identifying and addressing risks associated with their supervised institutions' crypto-related activities.

We applied internal control principles promulgated by the GAO (the Green Book) to guide our work when appropriate. For example, we considered internal controls standards, and activities, related to (1) identifying, analyzing, and responding to risks and (2) implementing control activities such as documentation of responsibilities through policies.

Appendix 2

Acronyms and Abbreviations

Crypto Asset Working Group	Crypto Asset Risks Interdivisional Working Group
DCP	Division of Depositor and Consumer Protection
DRR	Division of Resolutions and Receiverships
FDIC	Federal Deposit Insurance Corporation
FFI	Failing or failed institutions
FIL	Financial Institution Letter
FRB	Board of Governors of the Federal Reserve System
GAO	United States Government Accountability Office
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
RD memo	Regional Director memorandum
RMS	Division of Risk Management Supervision
WO	Washington Office



Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Division of Risk Management Supervision

TO: Terry L. Gibson
Assistant Inspector General, Audits, Evaluations, and Cyber
Office of Inspector General

FROM: Doreen R. Eberley DOREEN
EBERLEY Digitally signed by
Doreen R. Eberley
Date: 2023.09.27
14:00:00 -0400
Director, Division of Risk Management Supervision

DATE: September 27, 2023

RE: Response to Draft Evaluation Report
FDIC Strategies Related to Crypto Asset Risks (No. 2022-007)

BACKGROUND

The FDIC has completed its review of the Office of Inspector General's (OIG) draft evaluation report entitled, *FDIC Strategies Related to Crypto Asset Risks (No. 2022-007)*, provided on August 31, 2023 ("draft report"). FDIC concurs with the OIG's two recommendations, and provides a response to the recommendations below, including a summary of management's planned actions.

FDIC'S APPROACH TO ENGAGING WITH BANKS ON CRYPTO-RELATED ACTIVITIES

From the perspective of bank regulators, before banks engage in new or rapidly evolving activities, such as those related to the crypto-asset arena, it is important that they understand that the activity is permissible under applicable laws and regulations; that the activity can be conducted in a safe and sound manner; that the bank has put in place appropriate measures and controls to identify and manage the novel risks associated with those activities; and that the bank complies with all relevant laws and regulations, including those related to anti-money laundering/countering the financing of terrorism, and consumer protection. As the OIG points out in its report, the crypto-asset sector has proven to be highly volatile and has exhibited a number of risks to financial stability and institutions, including contagion risks due to high levels of interconnectedness within the sector.

As the crypto-asset sector grew rapidly in 2021 and early 2022, banking regulators recognized that there was also an increasing interest by some banks to engage in crypto-asset activities. The FDIC had been generally aware of the interest in crypto-asset related activities through its normal supervision process, but as interest accelerated, the FDIC recognized that there was insufficient information on which banks had been engaging in, or were interested in engaging in, crypto-related activities. To address that gap, and in consideration of various safety and soundness, consumer protection, and financial stability concerns, the FDIC issued Financial Institution Letter, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022) in April

FDIC Comments

2022, asking FDIC-supervised institutions to notify the FDIC of the crypto-related activities in which they were engaged or intended to engage.¹ FIL-16-2022 described some of the crypto-related risks about which the FDIC was concerned and indicated that the FDIC would provide supervisory feedback related to the planned or ongoing activities.

Subsequently, significant events, bankruptcies, and volatility in the crypto-asset industry exposed a number of vulnerabilities in the crypto-asset sector. For example, the May 2022 Terra USD collapse; the July 2022 bankruptcies of Three Arrows Capital (3AC), Voyager, and Celsius; the November 2022 FTX bankruptcy; and the significant price decline of Bitcoin (BTC) in 2022 from over \$47,000 to less than \$17,000.² Some of these disruptions involved consumers being unable to access their funds. In addition, it became evident that false and misleading statements, either direct or implied, by crypto-asset entities concerning the availability of deposit insurance for a given crypto-asset product violated the law, and could give consumers the impression that crypto-asset products are protected by FDIC deposit insurance, when they are not.³

In July 2022, the FDIC issued a fact sheet for consumers regarding deposit insurance⁴ and an advisory reminding insured banks of the risks that could arise related to misrepresentations of deposit insurance.⁵ While not specific to crypto-assets, the FDIC Board of Directors approved a final rule on May 17, 2022, to help address instances in which firms misrepresent the availability of deposit insurance in violation of the law.⁶ Also, on December 13, 2022, the FDIC Board of Directors issued for public comment a proposed rule to amend its regulations on use of the official FDIC sign and to clarify the FDIC regulation regarding misrepresentations of deposit insurance. This proposed rule also adds crypto-asset to the definition of non-deposit product.⁷ The volatility in the crypto-asset sector continued as 2022 unfolded, including a rapid deterioration in and ultimate bankruptcy of a large crypto-asset firm.⁸

The banking regulators had been observing and discussing the risks posed by the crypto-asset sector, and determined to issue interagency guidance regarding those risks. In January 2023, the FDIC, the Board of Governors of the Federal Reserve (Federal Reserve), and the Office of the Comptroller of the Currency (OCC) released a joint statement on crypto-asset risks to banking organizations (see FIL-01-2023, *Joint Statement on Crypto-Asset Risks to Banking Organizations*, issued January 5, 2023).⁹ The statement describes the risks to banking

¹ See <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>

² See, for example,

<https://www.washingtonpost.com/business/2022/07/06/voyager-bankruptcy-three-arrows/> and <https://www.washingtonpost.com/business/2022/07/13/crypto-bankruptcy-celsius-depositors/> and <https://www.nytimes.com/2022/11/11/business/ftx-bankruptcy.html> and <https://coinmarketcap.com/currencies/bitcoin/>

³ See <https://www.fdic.gov/news/press-releases/2022/pr22060.html>

⁴ See <https://www.fdic.gov/news/press-releases/2022/pr22058.html>

⁵ See <https://www.fdic.gov/news/financial-institution-letters/2022/fil22035.html>

⁶ See <https://www.fdic.gov/news/financial-institution-letters/2022/fil22021.html>

⁷ See <https://www.fdic.gov/news/financial-institution-letters/2022/fil22052.html>

⁸ See, for example, <https://www.nytimes.com/2022/11/11/business/ftx-bankruptcy.html> and <https://www.wsj.com/articles/crypto-crisis-a-timeline-of-key-events-11675519887>

⁹ See <https://www.fdic.gov/news/financial-institution-letters/2023/fil23001.html>

FDIC Comments

organizations and reminds banking organizations that they 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.

Also, in February 2023, the FDIC, Federal Reserve, and OCC issued a *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities* (see FIL-08-2023, issued on February 23, 2023).¹⁰ The statement highlights key liquidity risks associated with certain sources of funding from crypto-asset-related entities that banking organizations should be aware of. The statement reminds banking organizations to apply existing risk management principles and provides examples of practices that could be effective. The agencies also continue to emphasize that 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.¹¹

The FDIC has actively engaged with institutions that have advised the FDIC of their activities or plans pursuant to FIL-16-2022. In what appears to be a product of changing market conditions (e.g., crypto-asset firm bankruptcies and disruptions described above, challenging macroeconomic conditions, crypto-asset service providers exiting certain business lines), a number of FDIC-supervised institutions have provided updates on previously planned activities and subsequently notified the FDIC that they no longer plan to pursue crypto-related activities. The majority of banks that received pause letters have notified the FDIC that they are no longer actively pursuing crypto-related activity.¹²

CONTEXT REGARDING FDIC ENTERPRISE RISK MANAGEMENT

The FDIC carries out its mission by, among other things, supervising and examining financial institutions for safety and soundness and consumer protection. As part of its Enterprise Risk Management (ERM) function, the FDIC maintains an enterprise-wide Risk Inventory, which is a comprehensive, detailed list of risks that could hamper the FDIC's ability to achieve its goals and objectives. The risk attributes captured in the Risk Inventory include all the components from the GAO Standards for Internal Control in the Federal Government (Green Book) related to risk assessments that are outlined in the OIG draft evaluation report.

The Green Book outlines that a risk assessment "assesses the risk facing the entity as it seeks to achieve its objectives."¹³ The risk attributes captured in the Risk Inventory include: identifying the risk, existing controls to mitigate the risk, impact, likelihood, residual risk, and planned mitigations, among other things. The FDIC has identified risks related to staying abreast of

¹⁰ See <https://www.fdic.gov/news/financial-institution-letters/2023/fil23008.html>.

¹¹ See also, FIL 5-2015, *Statement on Providing Banking Services*, issued January 28, 2015.

¹² In the draft report's discussion of banks that received pause letters, the draft report states that some banks have not received any supervisory feedback. In those instances, banks are either no longer actively pursuing crypto-related activity or banks have: not provided information requested by the FDIC; materially revised the proposed activities and the FDIC has requested updated information; or the proposed activities are broad, complex, and significant (for which FDIC staff are actively working on providing supervisory feedback).

¹³ See GAO-14-704G Federal Internal Control Standards, page 7.

FDIC Comments

industry trends and emerging technology, as well as ongoing efforts related to crypto-assets as controls for those risks.

FDIC MANAGEMENT RESPONSE TO RECOMMENDATIONS

FDIC concurs with the recommendations.

Recommendation 1: OIG recommends that the Crypto Asset Risks Interdivisional Working Group:

1. Establish a plan with timeframes for assessing risks pertaining to crypto-related activities by:
 - a) Continuing to identify and document crypto-asset risks,
 - b) Performing and documenting an analysis of the identified risks to estimate their significance, and
 - c) Developing and documenting strategies to address crypto-asset risks.

Planned Action: The FDIC concurs with this recommendation. The FDIC will utilize the ERM program to continue to identify and document risks that may face the FDIC in achieving its mission associated with supervising banks pursuing crypto-related activities, including the significance of those risks, and as appropriate, will identify any additional supervisory strategies to encourage bank management to appropriately manage risks to the bank.

Estimated Completion Date: The divisions that are members of the Interdivisional Working will provide a memorandum to the Chief Risk Officer documenting the risk assessment by January 30, 2024.

Recommendation 2: OIG recommends that the Director of the Division of Risk Management Supervision (RMS): Update and clarify the supervisory feedback process to (a) establish an expected timeframe for reviewing information and responding to FDIC-supervised institutions pursuant to the Financial Institution Letter and (b) describe what constitutes the completion of its review of its supervised institutions' crypto-related activities.

Planned Action: The FDIC concurs with this recommendation. The RMS Director, in coordination with the Director of the Division of Depositor and Consumer Protection, and in consultation with the Legal Division as appropriate, will update joint internal processes to include instructions for establishing expected timeframes for: 1) reviewing additional information after it is requested and received by the FDIC, and 2) responding to FDIC-supervised institutions after such date that the FDIC determines sufficient information has been received. Those instructions may allow for consideration of factors, such as the complexity of the activities or proposed activities, when establishing expected timeframes. In addition, the FDIC will update joint internal processes to outline expectations for communicating to an institution what constitutes the completion of the case-specific crypto-related activity review process.

FDIC Comments

Estimated Completion Date: Internal processes will be updated via a joint regional director memorandum that will be issued by January 30, 2024.

Appendix 4

Summary of the FDIC's Corrective Actions

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved: ^a Yes or No	Open or Closed ^b
1	The FDIC will utilize the ERM program to continue to identify and document risks that may face the FDIC in achieving its mission associated with supervising banks pursuing crypto-related activities, including the significance of those risks, and as appropriate, will identify any additional supervisory strategies to encourage bank management to appropriately manage risks to the bank.	January 30, 2024	\$0	Yes	Open
2	The RMS Director, in coordination with the Director of the Division of Depositor and Consumer Protection, and in consultation with the Legal Division as appropriate, will update joint internal processes to include instructions for establishing expected timeframes for: 1) reviewing additional information after it is requested and received by the FDIC, and 2) responding to FDIC-supervised institutions after such date that the FDIC determines sufficient information has been received. Those instructions may allow for consideration of factors, such as the complexity of the activities or proposed activities, when establishing expected timeframes. In addition, the FDIC will update joint internal processes to outline expectations for communicating to an institution what constitutes the completion of the case-specific crypto-related activity review process.	January 30, 2024	\$0	Yes	Open

^a Recommendations are resolved when —

1. Management concurs with the recommendation, and the OIG agrees the planned corrective action is consistent with the recommendation.
2. Management does not concur or partially concurs with the recommendation, but the OIG agrees that the proposed corrective action meets the intent of the recommendation.
3. For recommendations that include monetary benefits, management agrees to the full amount of OIG monetary benefits or provides an alternative amount and the OIG agrees with that amount.

^b Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.



Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★ ★ ★ ★ ★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our [Hotline](#) or call 1-800-964-FDIC.

FDIC OIG website

www.fdicig.gov

X, formerly known as Twitter

@FDIC_OIG



www.oversight.gov/

Appendix B

History Associates Inc. v. FDIC, No. 1:24-cv-1857-ACR (D.D.C.)

FDIC's Redacted Pause Letters

November 22, 2024

DOCUMENT 1

FDIC Federal Deposit Insurance Corporation
 Dallas Regional Office
 600 North Pearl Street, Suite 700, Dallas, Texas
 (214) 754-0098 FAX (972) 761-2082

Division of Risk Management Supervision
 Division of Depositor and Consumer Protection

SENT VIA SECURED ELECTRONIC MAIL

March 11, 2022

The Board of Directors
 [REDACTED]
 [REDACTED]

Subject: Proposed New FinTech Product [REDACTED]

Dear Members of the Board:

This office received [REDACTED] submission [REDACTED] that provided high-level information relating to the subject product. The proposed product is [REDACTED]. However, at this time the FDIC has not yet determined what, if any, regulatory filings will be necessary for a bank to engage in this type of activity. As a result, we respectfully ask that you pause all crypto asset-related activity. The FDIC will notify all FDIC-supervised banks at a later date when a determination has been made on the supervisory expectations for engaging in crypto asset-related activity, including the need for any regulatory filings.

You may direct questions on this matter to [REDACTED]

[REDACTED] As a reminder, written correspondence should be addressed to Kristie Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>. If there are any questions about the Secure Email process, please contact [REDACTED] or me at [REDACTED].

Sincerely,

Eric T. Guyot (Signed)

Eric T. Guyot
 Assistant Regional Director

cc: Federal Reserve Bank of Atlanta
 [REDACTED]

DOCUMENT 2



FEDERAL DEPOSIT INSURANCE CORPORATION
10 10th Street NE, Suite 800
Atlanta, Georgia 30309-3849

Atlanta Regional Office
Division of Risk Management Supervision
(678) 916-2200

March 15, 2022

Via Secure Email

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Subject: [REDACTED]
[REDACTED]

Based on recent discussions with you and your management team, as well as review of documentation provided by the bank, [REDACTED] intends to offer bank clients [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Please notify us of any material change from the arrangement as described to the FDIC.

[REDACTED] Thereafter, the FDIC may have additional questions to clarify the bank's proposed activities prior to expanding the service to ensure the bank is operating in safe and sound manner.¹

If you have any questions concerning this letter, please contact [REDACTED]
[REDACTED]

Sincerely,

Frank R. Hughes
Acting Regional Director

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

DOCUMENT 3



Federal Deposit Insurance Corporation
Division of Risk Management Supervision
350 5th Avenue, New York, NY 10018

New York Regional Office

March 25, 2022

Board of Directors

c/o [REDACTED]

Subject: [REDACTED]

Dear Members of the Board:

[REDACTED]

[REDACTED] conference call to discuss
[REDACTED] proposal with representatives from the [REDACTED]
[REDACTED] understand, as a result of this conference call, that [REDACTED]

The FDIC has a number of questions based on the information provided to date. We expect you to satisfactorily address them (in advance of implementation) to ensure the bank is operating in a safe and sound manner.¹ To assist the FDIC [REDACTED] we will be sending, under separate cover, (i) the [REDACTED] that have not yet been satisfactorily addressed and (ii) additional questions and document requests that will need to be addressed.

Written correspondence should be addressed to Jessica A. Kaemingk, Acting Regional Director, FDIC, New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (<https://secureemail.fdic.gov/>) using the following email address: NYMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

[REDACTED]
Board of Directors

Page 2 of 2

If you have any questions, please contact Assistant Regional Director Steven P. Slovinski
at [REDACTED].

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]
Federal Reserve Bank of New York

DOCUMENT 4



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 350 5th Avenue, New York, NY 10018

New York Regional Office

March 25, 2022

Board of Directors

[REDACTED]

Subject: Activity Related to [REDACTED]

Dear Board Members:

[REDACTED] met with the FDIC and notified the FDIC of a new planned product, [REDACTED]

[REDACTED] along with other bank management, participated in a conference call to discuss [REDACTED] with representatives from the FDIC [REDACTED] with a follow-up call on [REDACTED] The regulators understand, as a result of these discussions, [REDACTED]

The FDIC has a number of questions based on the information provided to date. We expect you to satisfactorily address them (in advance of implementation) to ensure the bank will be engaging in this new activity in a safe and sound manner.¹ To assist [REDACTED] we will be sending, under separate cover, (i) the questions [REDACTED] that have not yet been satisfactorily addressed; and (ii) additional questions and document requests that will need to be addressed prior to launch [REDACTED].

Written correspondence should be addressed to Jessica A. Kaemingk, Acting Regional Director, FDIC, New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (<https://secureemail.fdic.gov/>) using the following email address: NYMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

[REDACTED]
Board of Directors

Page 2 of 2

If you have any questions, please contact Assistant Regional Director Steven P. Slovinski
at [REDACTED]

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

[REDACTED]

DOCUMENT 5



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
 Phone (312) 382-7500
 Fax (312) 382-6901

April 5, 2022

Board of Directors
 [REDACTED]
 [REDACTED]

Subject: Activity Related to [REDACTED]

Dear Board Members:

[REDACTED] the Federal Deposit Insurance Corporation (FDIC), [REDACTED] management team participated in a virtual meeting to discuss crypto-asset [REDACTED]. [REDACTED] Subsequent to that meeting, the FDIC [REDACTED] received additional documentation regarding the bank's agreements, risk assessment, and due diligence related to this new service.

The FDIC has a number of questions based on the information provided to date. Those include questions with respect to the permissibility of this activity, including what legal analysis the bank performed related to permissibility and to assess compliance with Part 362 of the FDIC Rules and Regulations. Those also include questions with respect to safety and soundness¹ related to this activity and consumer protection issues. The FDIC plans to perform a detailed review of this activity and will seek further information with respect to those questions at the upcoming [REDACTED] examination. Until [REDACTED] should not expand the service to additional customers.

If you have any questions, please contact Deputy Regional Director Christopher J. Newbury at [REDACTED]

Sincerely,

GREGORY Digitally signed by
BOTTONE GREGORY BOTTONE
 Date: 2022.04.05
 12:03:16 -04'00'
 Gregory P. Bottone
 Regional Director

cc: [REDACTED]

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

DOCUMENT 6



Dallas Regional Office
 600 North Pearl Street, Suite 700
 Dallas, Texas 75201
 (214) 754-0098 FAX (972) 761-2082

April 15, 2022

The Board of Directors

[REDACTED]
 [REDACTED]
 [REDACTED]

Subject: Proposed [REDACTED]

Dear Members of the Board:

We received [REDACTED] submission [REDACTED] that provided high-level information related to the subject [REDACTED]. The proposed product will [REDACTED]

[REDACTED] However, at this time the FDIC has not yet determined what, if any, regulatory filings will be necessary for a bank to engage in this type of activity. As a result, we respectfully ask that you pause all crypto asset-related activity. The FDIC will notify all FDIC-supervised banks at a later date when a determination has been made on the supervisory expectations for engaging in crypto asset-related activity, including the need for any regulatory filings. Refer to the Financial Institution Letter issued on April 7, 2022, FIL-16-2022-Notification of Engaging in Crypto-Related Activities, for additional information.

Please direct questions on this matter to [REDACTED] As a reminder, written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DAI.MailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>. If you prefer to send correspondence via mail, please use the Dallas Regional Office address noted in the letterhead. If there are any questions about the Secure Email process, please contact [REDACTED].

Sincerely,

Signed by Joseph A. Meade

Joseph A. Meade
 Assistant Regional Director

cc: Federal Reserve Bank of Kansas City
 [REDACTED]

DOCUMENT 7



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 350 5th Avenue, New York, NY 10018

New York Regional Office

April 22, 2022

Board of Directors

[REDACTED]

Subject: [REDACTED]

Dear Members of the Board:

[REDACTED]

[REDACTED] We appreciate the transparency [REDACTED] over the past several months in keeping us informed as the bank has conducted due diligence and explored its entry into the digital asset space. This letter serves as a follow-up to what was discussed in regards to [REDACTED] and FDIC New York Regional Office staff.

[REDACTED] participated in a [REDACTED] conference call to discuss the [REDACTED] proposal with representatives from the FDIC, [REDACTED]

[REDACTED] The Federal regulators understand, as a result of this conference call, that [REDACTED]

The FDIC has a number of questions based on the information provided to date. We expect [REDACTED] to address those (in advance of implementation) to ensure [REDACTED] operating in a safe and sound manner.¹ To assist the FDIC and the other Federal regulators in [REDACTED], we will be sending, under separate cover, (i) the questions regarding [REDACTED] have not yet been satisfactorily addressed and (ii) additional questions and document requests that will need to be addressed. In addition to this outreach, we may reach out [REDACTED] with questions to gain an understanding of how the bank will ensure continued safe and sound operation as this activity is implemented.

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

[REDACTED]
Board of Directors

Page 2 of 2

Written correspondence should be addressed to Jessica A. Kaemingk, Acting Regional Director, FDIC, New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (<https://secureemail.fdic.gov/>) using the following email address: NYMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

If you have any questions, please contact Assistant Regional Director Ashley M. Amicangioli at [REDACTED]

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]
[REDACTED]

DOCUMENT 8



Dallas Regional Office
 600 North Pearl Street, Suite 700
 Dallas, Texas 75201
 (214) 754-0098 FAX (972) 761-2082

April 25, 2022

Board of Directors

[REDACTED]

Via Secure Email

Members of the Board:

[REDACTED] the FDIC, [REDACTED] met with [REDACTED]
 [REDACTED], participated in the meeting to discuss the
 functionality of the product [REDACTED]
 [REDACTED] versions of the product, [REDACTED]
 [REDACTED] and subsequently, FDIC has received revised information outlining three models [REDACTED]

In our letter to you [REDACTED] the FDIC stated it has a number of questions based on the discussion and information provided to date. The initial questions are attached and we request responses [REDACTED]. As noted in our prior letter, we expect you to satisfactorily address these and any subsequent questions (in advance of implementation) to ensure the bank is operating in a safe and sound manner.¹ This is consistent with FIL-16-2022 which requests that institutions provide information necessary to allow the agency to assess the safety and soundness, consumer protection, and financial stability implications of such activities.

Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

Kristie Elmquist
 Regional Director

Attachment

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations

1. **Structure** [REDACTED].
 - a. Describe the activities conducted by [REDACTED] the assets held by [REDACTED] the relationship [REDACTED]
 - b. Describe the [REDACTED] processes for decision-making, key participants, and key personnel. In your response, indicate [REDACTED]
 - c. Describe what role, [REDACTED]
 - d. Describe what role, [REDACTED]
 - e. Provide the terms of [REDACTED] documents that describe the terms [REDACTED] Identify the party responsible for [REDACTED]
 - f. Explain in detail [REDACTED] Identify all persons that control 5 percent or more [REDACTED] and provide the percentage controlled.
 - g. Explain any dispute resolution processes [REDACTED]
 - h. Provide a list of the fees [REDACTED] and estimated expenses moving forward. In your response, please clarify what the fees are for [REDACTED]
 - i. Discuss the permissibility [REDACTED] under section [REDACTED] Federal Deposit Insurance Act, [REDACTED] the FDIC Rules and Regulations, [REDACTED]
 - j. Clarify whether [REDACTED]
 - k. Describe what involvement, if any, [REDACTED]
 - l. Identify the steps [REDACTED]
 - m. Describe key third-party relationships [REDACTED]
 - n. [REDACTED] business-to-business payments, merchant payments, [REDACTED] to ensure privacy, confidentiality and/or data security for the different types of customers and their data.
 - o. Explain any restrictions in place regarding the use of data [REDACTED] In your response identify the parties with access to such data and the type(s) of data they

can access and any controls monitoring the use of such data. Explain the rights and responsibilities with respect to privacy and/or data security violations.

- p-
■
■
■
■

2. [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

3. Accounting.

- Explain how funds _____ the balance sheet _____.
- Explain whether and how _____ on the balance sheet _____.
- Explain whether reserves will be held in _____

_____.
- Provide example general ledger entries _____

_____. Please provide a chart depicting the flow of funds.

4. Exposure to [REDACTED]

- a. [REDACTED] describe any controls in place [REDACTED]
[REDACTED]
- b. Explain the liability, if any, [REDACTED]
[REDACTED]

5. Risk Management and Controls.

- a. Describe the role of the board in reviewing and approving [REDACTED]
- i. Explain the process [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- b. [REDACTED] risk assessment and due diligence [REDACTED]
- key personnel [REDACTED]
- c. [REDACTED] relevant expertise needed [REDACTED]
- [REDACTED]
- [REDACTED] limitations on customer activity [REDACTED]
- [REDACTED]
- [REDACTED] systems or procedures to allow for this activity.
- [REDACTED] risk management systems, processes, and controls [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- g. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] mitigate risks related to security and privacy.
- i. [REDACTED] mitigate operational risk [REDACTED]
- [REDACTED]
- j. [REDACTED]
- [REDACTED]
- k. [REDACTED] efforts to conduct due diligence and assess the risks [REDACTED]
- [REDACTED]
- l. [REDACTED]
- [REDACTED]
- [REDACTED]
- m. [REDACTED]
- [REDACTED]
- [REDACTED]
- n. Describe and provide documentation of vulnerability analysis [REDACTED]
- [REDACTED]

Settlement: [REDACTED]
[REDACTED]
[REDACTED]

- [illegible]

-
- | Government | Percentage |
|---------------------|------------|
| Current government | 80% |
| Previous government | 20% |

[illegible]

- h. Describe any representations that [REDACTED] is making or plans to make regarding [REDACTED]
[REDACTED]
- i. [REDACTED]
- j. Identify the consumer data that will be shared with [REDACTED] as well as any controls in place to protect PII and limit sharing. In your response, indicate whether any PII will be stored [REDACTED]
[REDACTED]

DOCUMENT 9



Dallas Regional Office
 600 North Pearl Street, Suite 700
 Dallas, Texas 75201
 (214) 754-0098 FAX (972) 761-2082

SENT VIA SECURED ELECTRONIC MAIL

May 4, 2022

The Board of Directors
 [REDACTED]
 [REDACTED]
 [REDACTED]

Subject: Proposed Crypto Asset Capability

Dear Members of the Board:

This office received [REDACTED] that provided high-level information about the bank's intent to provide a crypto asset capability [REDACTED]. We thank you for your timely notification as requested by Financial Institution Letter (FIL-16-2022) dated April 7, 2022.

At this time the FDIC has not yet determined what, if any, regulatory filings will be necessary for a bank to engage in this type of activity. As a result, we respectfully ask that you not implement this product, while we consider this crypto asset-related activity.

As we review your proposed activity, we will continue to correspond with your institution regarding additional information requests to aid us in our assessment of the activity. In the meantime, you may direct questions on this matter to [REDACTED]. Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

/s/ J. Mark Love

J. Mark Love
 Assistant Regional Director

cc: Federal Reserve Bank of Dallas
 [REDACTED]

DOCUMENT 10



Dallas Regional Office
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

May 13, 2022

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: [REDACTED]

Dear Members of the Board:

By letter dated [REDACTED] advised the FDIC and the [REDACTED] of the Bank's intent to offer Bank customers [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

By letter dated [REDACTED] additional information was received [REDACTED] this service, and a brief conference call [REDACTED] By letter dated [REDACTED], the FDIC and [REDACTED] outlined certain information [REDACTED]
[REDACTED]

On April 7, 2022, the FDIC issued a Financial Institution Letter, FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. That FIL is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

[REDACTED]
[REDACTED]
[REDACTED]

The FDIC continues to review [REDACTED] and various questions remain outstanding, including with respect to the legal permissibility of this activity, the potential applicability of part 362 of the FDIC Rules and Regulations, and safety and soundness and consumer protection principles. Consistent with the procedures outlined in FIL-16-2022, the FDIC will make future information requests to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service to additional customers.

[REDACTED]
[REDACTED]

If you have any questions, please contact Assistant Regional Director Cindy Scott at [REDACTED]. Written correspondence should be addressed to my attention at the Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

Kristie K. Elmquist
Regional Director

[REDACTED]

DOCUMENT 11

**Federal Deposit Insurance Corporation**Division of Risk Management Supervision and Division of Depositor and Consumer Protection
350 5th Avenue, New York, NY 10018

New York Regional Office

June 22, 2022

Board of Directors
[REDACTED]**Subject: [REDACTED] Notice to Engage in Digital Asset Activities under FIL-16-2022**

Dear Members of the Board:

We received the subject correspondence [REDACTED] in response to Financial Institution Letter 16-2022, notifying the FDIC of the Bank's intent to engage in activities involving digital assets. New York Regional Office staff has met numerous times with Bank management over the past several months regarding these proposed activities. We appreciate management's efforts to keep us informed as the Bank has conducted due diligence and explored its entry into the digital asset space.

The FDIC has a number of questions regarding the activities based on the information provided to date. The FDIC plans to conduct a targeted review of the Bank's planned digital asset activities [REDACTED] to gain an understanding of how the Bank will ensure continued safe and sound operations and consumer protections, should these activities be implemented. A document request list related to this targeted review was provided under separate cover. The Bank should address these questions, in advance of implementation of the proposed activities, in order for the FDIC to assess the safety and soundness of the proposed activities¹ and compliance with laws and regulations.

If you have any questions, please contact Assistant Regional Director Ashley M. Amicangioli at [REDACTED] or Assistant Regional Director Kara L. Ritchie at [REDACTED].

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

DOCUMENT 12



Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
Phone (312) 382-7500
Fax (312) 382-6901

June 27, 2022

Board of Directors
[REDACTED]

Subject: [REDACTED]

[REDACTED] Members of the Board:

By letter dated [REDACTED]
[REDACTED] advised the FDIC, in response to Financial Institution Letter 16-2022 (FIL-16-2022),¹ and [REDACTED] of the Bank's intent to offer Bank customers [REDACTED]

[REDACTED]

The FDIC continues to review [REDACTED] and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC will request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service.

If you have any questions, please contact [REDACTED]
[REDACTED] Written correspondence should be addressed to my attention at the Chicago Regional Office, and sent as a PDF document through [REDACTED]

¹ On April 7, 2022, the FDIC issued FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. FIL-16-2022 is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil2016.html>.

the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address:
CHIMailRoom@FDIC.gov.

Sincerely,

Gregory P. Bottone
Regional Director

[REDACTED]

DOCUMENT 13



Federal Deposit Insurance Corporation
350 Fifth Avenue, Suite 1200, New York, NY 10118

New York Regional Office

June 30, 2022

Board of Directors
[REDACTED]

Subject: [REDACTED]

Dear Members of the Board:

[REDACTED]

In a letter dated [REDACTED] provided an overview of the program and due diligence activities in response to the FDIC Financial Institution Letter, FIL-16-2022, dated April 7, 2022 (FIL-16-2022). FIL-16-2022 explains the notification and supervisory feedback process concerning current or planned crypto-asset-related activity. On June 1, 2022, the Bank, the FDIC, and [REDACTED] discussed the program again. [REDACTED]

The FDIC continues to review [REDACTED] and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC will request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the bank refrain from expanding this service.

If you have any questions, please contact Assistant Regional Director Catherine H. Goni at [REDACTED]. Written correspondence should be addressed to my attention at the New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: NYMailroom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

[REDACTED]

[REDACTED]

DOCUMENT 14



Division of Risk Management Supervision
Division of Depositor and Consumer Protection

Dallas Regional Office
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

July 14, 2022

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: [REDACTED]

[REDACTED] Members of the Board:

By letter dated [REDACTED] provided notification pursuant to Financial Institution Letter-16-2022, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022), of its program offering customers [REDACTED]
[REDACTED]
[REDACTED]

On [REDACTED] the FDIC held a videoconference meeting, with members of the Bank's executive team to discuss [REDACTED]
[REDACTED] represented the Bank. Assistant Regional Director (ARD) J. Mark Love, ARD Cynthia Scott, ARD Akhtar Khan, and Case Manager [REDACTED] represented the FDIC.

During the meeting, [REDACTED] informed the FDIC that the program is live as of [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

The FDIC continues to review crypto-related activities and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC may request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service.

If you have any questions, please contact ARD Love at [REDACTED] Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

[REDACTED]
[REDACTED]

Page 2

Sincerely,

/s/ Kristie K. Elmquist

Kristie K. Elmquist
Regional Director

[REDACTED]

DOCUMENT 15

**FDIC**

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

Division of Risk Management Supervision
San Francisco Regional Office
(415) 546-0160

July 27, 2022

Board of Directors

[REDACTED]

Subject: Notification of Crypto-Related Activity

Dear Members of the Board:

By letter dated [REDACTED] notified the
FDIC and [REDACTED] that the
Bank will provide its customers [REDACTED]

[REDACTED]

On April 7, 2022, the FDIC issued a Financial Institution Letter, FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. That FIL is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

[REDACTED]

On [REDACTED] Safety and Soundness examination began. [REDACTED]
[REDACTED] examiners and bank management held an MS Teams Meeting to present an additional request list related to the proposed crypto activities. During the meeting, [REDACTED]

[REDACTED]

The FDIC continues to review [REDACTED] and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC has requested information as part of the examination process and may request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service to its customers.

If you have any questions, please contact RMS Assistant Regional Director David Wong at [REDACTED] or DCP Assistant Regional Director Matthew Sheeren 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 about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

Digitally signed by
KATHY MOE
Date: 2022.07.27
15:37:45 -0700
Kathy L. Moe
Regional Director

cc: [REDACTED]

DOCUMENT 16

**FDIC**

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

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

Sent via secure email to [REDACTED]

July 28, 2022

Board of Directors
 [REDACTED]

Subject: Notification of Engaging in Crypto-Related Activities

Dear Members of the Board:

On [REDACTED] submitted [REDACTED] draft three-year business plan (Plan) pursuant to FDIC's Financial Institution Letter-16-2022, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022). We also held a brief discussion with [REDACTED]

[REDACTED] As discussed during the call, the Plan [REDACTED]
 the bank's business model [REDACTED]

While the FDIC continues to review the bank's Plan pursuant to FIL-16-2022, in order to assess the safety and soundness and consumer protection implications of such activities, additional information is needed and questions remain outstanding. [REDACTED]

[REDACTED] it is essential for management to [REDACTED] prior to implementation to ensure planned activities and strategies are consistent with current laws, rules, and regulations, as well as safety and soundness and consumer protection principles. Examples of incomplete, but essential, elements that we request the opportunity to review, when available, include the following:

- Risk assessments [REDACTED].
- Due diligence [REDACTED]
- Policies and procedures [REDACTED]
- Project plans and cost benefit analysis [REDACTED].
- Formal succession plan [REDACTED].

Board of Directors

Page 2

- Draft contracts and legal agreements [REDACTED]
- Legal analysis of the permissibility of the proposed [REDACTED] under Part 362 of the FDIC's Rules and Regulations, including [REDACTED]
- Also with respect to [REDACTED]
- Banking services [REDACTED]
- Plans to expand [REDACTED] and expected impacts to the Community Reinvestment Act (CRA) performance,
- Any assessment of consumer protection risk [REDACTED]
- Analysis performed with respect to SEC Staff Accounting Bulletin No. 121 and proposed new products and services, and,
- Plans for ongoing monitoring and audit [REDACTED]

[REDACTED] Consistent with the procedures outlined in FIL-16-2022, the FDIC may make future information requests to assist us in reviewing the activities and providing any relevant supervisory feedback to the bank. Accordingly, until we complete our review, we request that the bank not proceed with planned activities, pending FDIC supervisory feedback, and that you continue to update us on developments in the bank's risk management framework and compliance management system.

If you have any questions related to Risk Management, please contact Assistant Regional Director Jaclyn Valderrama or [REDACTED] respectively. For questions related to Consumer Protection, please contact Assistant Regional Director Matthew Sheeren or [REDACTED] respectively. 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

Board of Directors
[REDACTED]

Page 3

portal (<https://securemail.fdic.gov/>) using the following e-mail address: SFMailRoom@fdic.gov.
Information about 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

cc: [REDACTED]

DOCUMENT 17



Federal Deposit Insurance Corporation
1100 Walnut Street, Suite 2100, Kansas City, MO 64106

Division of Risk Management Supervision

August 9, 2022

Board of Directors
[REDACTED]
[REDACTED]

Subject: [REDACTED]

Dear Members of the Board:

By letter dated [REDACTED] advised the FDIC of the bank's intent to offer customers [REDACTED] in response to FIL-16-2022.¹ [REDACTED]

On [REDACTED] the Bank discussed the [REDACTED] with the FDIC Division of Depositor and Consumer Protection – Kansas City Regional Office (RO). Follow-up discussions were held on [REDACTED] During the course of those discussions Bank management explained [REDACTED] By letter [REDACTED], additional information from the Bank was forwarded to the RO documenting [REDACTED]

The FDIC continues to review [REDACTED] and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC will make future information requests to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service to additional customers.

¹ On April 7, 2022, the FDIC issued a Financial Institution Letter, FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. That FIL is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

Case 1:24-cv-01857-ACR Document 26-1 Filed 12/06/24 Page 51 of 75

If you have any questions, please contact Assistant Regional Director Michele Sharp or Case Manager Nick Ellwanger at [REDACTED]. Written correspondence should be addressed to my attention at the Kansas City 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: KCMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,
James D. LaPierre
Regional Director

[REDACTED]

DOCUMENT 18



FEDERAL DEPOSIT INSURANCE CORPORATION
10 10th Street NE, Suite 800
Atlanta, Georgia 30309-3849

Atlanta Regional Office
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
(678) 916-2200

August 26, 2022

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Notification of Crypto-Related Activity

Dear Members of the Board:

On [REDACTED] the FDIC received [REDACTED] notification, in response to Financial Institution Letter (FIL), [FIL-16-2022, Notification of Engaging in Crypto-Related Activities](#), of the Bank's intent to engage in crypto-asset related activity by offering customers [REDACTED]. 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. [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] 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 such activities. To assess these risks, the FDIC is reviewing the notification and information provided, and is also assessing whether [REDACTED]
[REDACTED]
[REDACTED]

To assist in our review of the proposed activities, please provide the documentation referenced in the Appendix attached to this letter. We will review this documentation to assess the safety and soundness, consumer protection, and [REDACTED] stability implications of such activities as it is received and in conjunction with the safety and soundness examination [REDACTED]. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the Bank refrain from providing this service to its customers.

Please submit the information requested in the Appendix to the FDIC as a PDF file to ATLMailRoom@fdic.gov using the secure message center at <https://securemail.fdic.gov>. The

information should be submitted to this office by [REDACTED]. If you foresee any issues with meeting this deadline, please contact the individuals identified below.

If you have any questions related to Risk Management, please contact [REDACTED]
[REDACTED] If you have any questions related to Consumer
Protection, please contact [REDACTED]
[REDACTED].

Sincerely,

Frank R. Hughes
Acting Regional Director

cc: [REDACTED]

Appendix
Crypto-Related Activity Request List

Please provide the following documentation in relation to the proposed crypto-related activities:

1. All contracts (including any draft contracts that the 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. [REDACTED]
6. The Bank's permissibility analysis and determination with respect to each activity;
7. The Bank's analysis of SEC SAB 121 and its applicability;
8. Any cost-benefit analysis conducted;
9. Project plan for each activity;
10. [REDACTED]
14. [REDACTED]
15. Copies of consumer agreements, disclosures, and other terms and conditions related to each of the activities provided by or through the Bank and by third parties (draft or proposed);
16. Marketing materials, press releases, internal scripts, educational materials, and any other publicly distributed information related to each of the activities (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 consumers by, or through, the Bank in connection with each of the activities;

17. Strategic plan that details how crypto-asset activities achieve the objectives of the Board and any contingency plan, should the activities fail to achieve the objectives;
18. Implementation plan. For each activity, please include expected volumes, income projections used to determine whether the products are financially feasible, and any other analysis performed to support launching the products;
19. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activities;
20. Internal training materials related to the activities;
21. Policies and procedures that will govern each of the crypto-related activities, including those related to consumer compliance and complaint resolution (we acknowledge receipt of the policy outline previously submitted, this request is for the policies and procedures);
22. 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); and
23. [REDACTED]
24. Describe how the risk assessment was developed, what policies govern the structure/process for risk assessments, and which staff performed the risk assessment. Explain how the Bank determined the risk assessment scope is appropriate for all three product types collectively (trading, interest enhancement, and rewards).
25. [REDACTED]
 - a. [REDACTED]

[illegible]

DOCUMENT 19



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 Division of Depositor and Consumer Protection
 300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
 Phone (312) 382-7500
 Fax (312) 382-6901

September 9, 2022

Board of Directors
 [REDACTED]

Subject: Third-Party Crypto-Asset Activity

Dear Members of the Board:

On [REDACTED] submitted a notification of the Bank's intended crypto-asset activities in response to Financial Institution Letter-16-2022, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022). [REDACTED] also held a discussion with [REDACTED] regarding the proposed crypto-asset activities. As discussed during the call, [REDACTED]

The FDIC requests insured depository institutions provide sufficient information to assist the FDIC to assess the safety and soundness, consumer protection, and financial stability implications of crypto-asset activities. The FDIC requests the Bank provide the information in the attached list by [REDACTED] so that the FDIC may begin those assessments. If the requested information has not yet been developed, provide the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the requested information, we will determine whether additional information is necessary to complete the review of the activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the Bank not proceed with planned activities, pending FDIC supervisory feedback.

If you have any questions, please contact [REDACTED]. Written correspondence should be addressed to my attention at the Chicago Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: CHIMailRoom@FDIC.gov.

Sincerely,
 Gregory P. Bottone
 Regional Director

Enclosure – Crypto-Asset Activity Request List

cc: [REDACTED]
 Federal Reserve Bank of Chicago

Crypto-Asset Activity Request List

1. Strategic Plan that details how crypto-related activity achieves objectives of the Bank's Board and the Contingency Plan in the event the activity fails to achieve those objectives.
2. Project/Implementation plan including, but not limited to, expected volumes of activity or contemplated activity limits, cost benefit analysis including income projections used to determine whether the services are financially feasible, and any other analysis performed to support launching the services.
3. Risk assessments for all crypto-related services. Consideration should be made to Safety and Soundness, Information Technology, Anti-Money Laundering/Combating the Financing of Terrorism, and Consumer Compliance.
4. Vendor management due diligence documentation, and analysis for all vendors that will provide crypto-related technologies or services.
5. Board and committee minutes reflecting approval, discussion, analysis, and any documentation provided on the activity.
6. Draft contracts and legal agreements between the Bank and crypto-related third party vendors.
7. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution.
8. If not outlined in policies and procedures, the framework of assigned responsibilities and qualifications for those involved in day-to-day administration of digital asset activity, including internal controls responsibilities, and a description of oversight responsibilities, for example: management; staff; committees, including committee members; frequency of meetings; and collectively, their approval authority, and expertise required to be a committee member.
9. Draft marketing plans, including press releases, educational and training materials, and any other proposed public distributions.
10. Draft consumer agreements, disclosures, or other terms and conditions related to these activities provided by, or through, the Bank and by third parties.
11. Legal analysis of the permissibility of the proposed services under part 362 of the FDIC's Rules and Regulations, and [REDACTED]
12. Analysis performed with respect to SEC Staff Accounting Bulletin No. 121 and proposed services.
13. Plans for ongoing monitoring and audit of crypto-related products and services.

DOCUMENT 20



FEDERAL DEPOSIT INSURANCE CORPORATION
10 10th Street NE, Suite 800
Atlanta, Georgia 30309-3849

Atlanta Regional Office
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
(678) 916-2200

September 13, 2022

Sent via secure email

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Third-Party Crypto-Asset Activity

Dear Members of the Board:

On [REDACTED] we received [REDACTED] notification, in response to Financial Institution Letter (FIL), [FIL-16-2022, Notification of Engaging in Crypto-Related Activities](#), of the Bank's intent to offer customers [REDACTED]

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") promptly notify the appropriate FDIC Regional Director.

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 such activities. In order to begin those assessments, please provide the information in the attached list by November 14, 2022. If the requested information has not yet been developed, include the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the above-requested information, we will determine whether additional information is necessary to complete the review of the activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the Bank refrain from providing these services to its customers.

Board of Directors
[REDACTED]

Page 2 of 2

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 [REDACTED]

[REDACTED] Written correspondence should be addressed to my attention at the Atlanta Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: ATLMailRoom@fdic.gov.

Sincerely,

JOHN

Digitally signed
by JOHN VOGEL
Date: 2022.09.13
16:45:08 -04'00'John F. Vogel
Acting Regional Director

cc: [REDACTED]

Enclosure

Crypto-Asset Activity Request List

Documentation (Prospective):

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. The bank's permissibility analysis and determination with respect to the activity
 5. Bank's analysis of SEC SAB 121 and its applicability
 6. Cost-benefit analysis
 7. Project plan
 8. [REDACTED]
 9. [REDACTED]
 10. Description of any fees that will be charged to consumers related to the activity, and how they will be calculated. Also, describe if and how fees are split amongst the bank and any third parties involved in the activity.
 11. [REDACTED]
 12. [REDACTED]
 13. [REDACTED]
 14. [REDACTED]
 15. [REDACTED]
 16. [REDACTED]
 17. [REDACTED]
 18. [REDACTED]
 19. [REDACTED]
 20. [REDACTED]
 21. [REDACTED]
 22. [REDACTED]
- This includes providing an explanation of how any market price is determined and how the spread, if any, is calculated.
13. Consumer agreements, disclosures, and other terms and conditions related to the activities provided by or through the bank and by third parties (draft or proposed)
 14. 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 consumers by, or through, the bank in connection with activities.
 15. Any other due diligence materials.
 16. Strategic plan that details how crypto-asset activity achieves objectives of the board and the contingency plan should the activity fail to achieve the objectives.
 17. 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.
 18. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activity.
 19. Risk assessment(s) related to the activity.
 20. Internal training materials related to the activity.
 21. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution.
 22. 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).

DOCUMENT 21



FEDERAL DEPOSIT INSURANCE CORPORATION
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

Dallas Regional Office
Division of Risk Management Supervision
Division of Depositor and Consumer Protection

SENT VIA SECURE ELECTRONIC EMAIL

September 14, 2022

Board of Directors
[REDACTED]

Subject: Notification of Crypto-Asset Related Activity

Dear Members of the Board:

By email dated [REDACTED]
notified us of [REDACTED] intent to provide its customers [REDACTED]
[REDACTED]

As stated in FIL-16-2022, *Notification of Engaging in Crypto-Related Activities*, 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 such activities. In order to begin those assessments, please provide the information in the attached list **by November 14, 2022**. If the requested information has not yet been developed, please include the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the requested information, we will determine whether additional information is necessary to complete the review of the activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the bank refrain from providing this service to its customers.

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 [REDACTED]. Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

[REDACTED]

Page 2

Sincerely,

Kristie K. Elmquist
Regional Director

Attachment

cc: Federal Reserve Bank of Dallas

[REDACTED]

Crypto-Asset Activity Request List [REDACTED]

Documentation:

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. [REDACTED]
6. [REDACTED]
7. The bank's permissibility analysis and determination with respect to the activity
8. Bank's analysis of SEC SAB 121 and its applicability
9. Cost-benefit analysis
10. Project plan
11. [REDACTED]
12. Description of any fees that will be charged to consumers related to the activity, and how they will be calculated. Also, describe if and how fees are split amongst the bank and any third-parties involved in the activity.
13. [REDACTED]
14. [REDACTED]
15. Consumer 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)
16. 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 consumers by, or through, the bank in connection with activities.
17. Any other due diligence materials
18. Strategic plan that details how crypto-asset activity achieves objectives of the board and the contingency plan should the activity fail to achieve the objectives
19. 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.
20. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activity
21. Risk assessment(s) related to the activity
22. Internal training materials related to the activity

23. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution
24. 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).

DOCUMENT 22



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 25 Jessie Street at Ecker Square, Suite 2300
 San Francisco, CA 94105

[REDACTED]

Transmitted by Electronic Correspondence

October 17, 2022

[REDACTED]

RE: Notification of Crypto-Related Activities

Dear [REDACTED]:

On [REDACTED] we received your letter notifying the FDIC and [REDACTED] of your institution's involvement in crypto-related activities, in response 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.

[REDACTED]

After a review of the Bank's notification letter, we have determined that additional information is needed to further clarify the crypto-related activities being conducted [REDACTED] by the Bank.

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 such activities. To assist in the review of the Bank's crypto-related activities, please provide the documentation listed below within 30 days of the date of this letter.

- [REDACTED]

This letter is confidential and may not be disclosed or made public in any manner. Additional information regarding these confidentiality restrictions may be found both in Part 309 of the FDIC Rules and Regulations and Chapter 167 Section 2 of Massachusetts General Law. Please notify regulators immediately if you receive a subpoena or other legal process calling for the production of this letter or a description of its content.

[REDACTED]

Page 2

- [REDACTED] Provide supporting documentation and analysis. Include financial statement disclosures concerning these activities.
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Until we complete our review, we request the Bank refrain from [REDACTED]
[REDACTED] When we have completed our review, we will provide the institution with relevant supervisory feedback, as appropriate.

Please notify us of any material changes in these activities or intent to engage in other crypto-related activities. 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). Questions should be directed to FDIC [REDACTED]
[REDACTED]

Sincerely,

/s/ Kathy L. Moe

Kathy L. Moe
Regional Director
Federal Deposit Insurance Corporation

[REDACTED]
[REDACTED]

DOCUMENT 23


FDIC

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

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

Sent via secure email

October 21, 2022

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Notification of Engaging in Crypto-Related Activities

Dear Members of the Board:

During a virtual meeting held on [REDACTED]
[REDACTED] and other bank personnel presented and discussed the bank's [REDACTED]
[REDACTED] with staff of the FDIC and [REDACTED]. During the meeting,
bank management presented an overview of the [REDACTED] activity to offer bank
customers [REDACTED]. They also
discussed management's risk assessment; the extent of contractual agreements; [REDACTED]
[REDACTED]
planned timeframe for implementation; the extent of [REDACTED]
[REDACTED]

On [REDACTED], during a virtual meeting, bank management provided an update to FDIC and
[REDACTED] staff on the project and their ongoing due diligence. Bank management also provided
additional documents and information on [REDACTED] in response to follow-
up requests from the FDIC. On [REDACTED]
notified [REDACTED] that the project had [REDACTED]
[REDACTED] as part of the bank's ongoing due diligence.

On [REDACTED] 2, 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 and outlined a supervisory feedback process concerning a bank's current or
planned crypto-asset related activity. The FIL is available at
<https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>. 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 such
activities. On [REDACTED] the FDIC submitted a list of requested information to the bank,

Board of Directors
[REDACTED]

Page 2

which is currently under review as part of the examination that began on [REDACTED]. When we have completed our review, the FDIC will provide the bank with relevant supervisory feedback, as appropriate. Until we complete our review, we request that the bank refrain from providing this service to its customers.

Please notify us during our review period if there are any material changes in the planned service, the status of this project, or its planned implementation, to ensure that the bank is operating in a safe and sound manner and in compliance with consumer protection regulations.

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 related to Risk Management, please contact Assistant Regional Director Jaclyn Valderrama at [REDACTED] or [REDACTED]. For questions related to Consumer Protection, please contact Assistant Regional Director Matthew Sheeren at [REDACTED] or Review Examiner Rolin Thomas 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 about 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

cc: [REDACTED]

Federal Reserve Bank of San Francisco

Appendix C

History Associates Inc. v. FDIC, No. 1:24-cv-1857-ACR (D.D.C.)

FDIC's Redacted Pause Letters

January 3, 2025

DOCUMENT 1

FDIC Federal Deposit
Insurance Corporation
Dallas Regional Office
600 North Pearl Street, Suite 700, Dallas, Texas
(214) 754-0098 FAX (972) 761-2082

Division of Risk Management Supervision
Division of Depositor and Consumer Protection

SENT VIA SECURED ELECTRONIC MAIL

March 11, 2022

The Board of Directors
[REDACTED]

Subject: Proposed New FinTech Product [REDACTED]

Dear Members of the Board:

This office received President and Chief Executive Officer [REDACTED] submission on February 25, 2022, that provided high-level information relating to the subject product. The proposed product is apparently an avenue for bank customers to engage in crypto asset activity, specifically Bitcoin transactions, through a third-party arrangement. However, at this time the FDIC has not yet determined what, if any, regulatory filings will be necessary for a bank to engage in this type of activity. As a result, we respectfully ask that you pause all crypto asset-related activity. The FDIC will notify all FDIC-supervised banks at a later date when a determination has been made on the supervisory expectations for engaging in crypto asset-related activity, including the need for any regulatory filings.

You may direct questions on this matter to Case Manager [REDACTED] at [REDACTED] or me at [REDACTED]. As a reminder, written correspondence should be addressed to Kristie Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>. If there are any questions about the Secure Email process, please contact Case Manager [REDACTED] or me at [REDACTED].

Sincerely,

Eric T. Guyot (Signed)

Eric T. Guyot
Assistant Regional Director

cc: Federal Reserve Bank of Atlanta
[REDACTED]

DOCUMENT 2



FEDERAL DEPOSIT INSURANCE CORPORATION
10 10th Street NE, Suite 800
Atlanta, Georgia 30309-3849

Atlanta Regional Office
Division of Risk Management Supervision
(678) 916-2200

March 15, 2022

Via Secure Email

President, [REDACTED]
[REDACTED]
[REDACTED]

Subject: [REDACTED] Internal Blockchain

Dear [REDACTED]

Based on recent discussions with you and your management team, as well as review of documentation provided by the bank, our understanding is that [REDACTED] intends to offer bank clients an internal blockchain-based, real-time payments service provided by [REDACTED]. You indicate that [REDACTED] is intended to enable real-time payments by tokenizing U.S. dollar deposits. The platform, as presented, is a closed-loop payments system that would involve the movement of tokens between existing [REDACTED] customers. Under this platform, all transactions and activities would remain within the bank, and no transactions would involve outside parties. We further understand that the bank has entered into a two-year agreement with [REDACTED] to provide this service.

Please notify us of any material change from the arrangement as described to the FDIC, including, but not limited to, expanding the service to include any clients, transactions or activities outside of the bank, such as through [REDACTED]. Thereafter, the FDIC may have additional questions to clarify the bank's proposed activities prior to expanding the service to ensure the bank is operating in safe and sound manner.¹

If you have any questions concerning this letter, please contact Case Manager [REDACTED] at [REDACTED] or by telephone at [REDACTED].

Sincerely,

Frank R. Hughes
Acting Regional Director

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

DOCUMENT 3



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 350 5th Avenue, New York, NY 10018

New York Regional Office

March 25, 2022

Board of Directors

[REDACTED]

Subject: Activity Related to [REDACTED]

Dear Members of the Board:

On [REDACTED], the [REDACTED], a [REDACTED] association of [REDACTED] institutions, was launched to further the adoption and interoperability of a [REDACTED] to facilitate the transfer of value on a blockchain. [REDACTED] is one of the [REDACTED] members of the [REDACTED]

[REDACTED] General Counsel and Corporate Secretary [REDACTED] along with leadership of the other [REDACTED] members, participated in a February 22, 2022 conference call to discuss the [REDACTED] and its proposal with representatives from the FDIC, the Board of Governors of the Federal Reserve System, and the Office of Comptroller of the Currency (collectively, Federal regulators). The Federal regulators understand, as a result of this conference call, that the [REDACTED] is currently drafting operating rules to govern transactions on the [REDACTED] blockchain network.

The FDIC has a number of questions based on the information provided to date. We expect you to satisfactorily address them (in advance of implementation) to ensure the bank is operating in a safe and sound manner.¹ To assist the FDIC and the other Federal regulators in the [REDACTED] review process, we will be sending, under separate cover, (i) the questions regarding the [REDACTED] that have not yet been satisfactorily addressed and (ii) additional questions and document requests that will need to be addressed.

Written correspondence should be addressed to Jessica A. Kaemingk, Acting Regional Director, FDIC, New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (<https://secureemail.fdic.gov/>) using the following email address: NYMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

[REDACTED]
Board of Directors

Page 2 of 2

If you have any questions, please contact Assistant Regional Director Steven P. Slovinski
at [REDACTED].

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]
Federal Reserve Bank of New York

DOCUMENT 4



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 350 5th Avenue, New York, NY 10018

New York Regional Office

March 25, 2022

Board of Directors
 [REDACTED]

Subject: Activity Related to [REDACTED] Bank Digital Deposit

Dear Board Members:

On October 12, 2021, [REDACTED] Bank met with the FDIC and notified the FDIC of a new planned product, the [REDACTED] Bank Digital Deposit ([REDACTED]) (f/k/a [REDACTED] Bank Digital Dollar).

President and Chief Executive Officer [REDACTED], along with other bank management, participated in a conference call to discuss [REDACTED] and its proposed launch with representatives from the FDIC and the [REDACTED] on October 12, 2021, with a follow-up call on November 15, 2021. The regulators understand, as a result of these discussions, that [REDACTED] represents an enhancement to the existing [REDACTED] technology. The [REDACTED] token design will also only enable transactions between qualifying [REDACTED] Bank commercial clients. [REDACTED], however, will operate on the [REDACTED] a decentralized public Blockchain, rather than on the [REDACTED], a private, permissioned Blockchain.

The FDIC has a number of questions based on the information provided to date. We expect you to satisfactorily address them (in advance of implementation) to ensure the bank will be engaging in this new activity in a safe and sound manner.¹ To assist in the [REDACTED] review process, we will be sending, under separate cover, (i) the questions regarding [REDACTED] that have not yet been satisfactorily addressed; and (ii) additional questions and document requests that will need to be addressed prior to launching [REDACTED].

Written correspondence should be addressed to Jessica A. Kaemingk, Acting Regional Director, FDIC, New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (<https://secureemail.fdic.gov/>) using the following email address: NYMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

[REDACTED]
Board of Directors

Page 2 of 2

If you have any questions, please contact Assistant Regional Director Steven P. Slovinski
at [REDACTED]

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]

DOCUMENT 5



Federal Deposit Insurance Corporation
Division of Risk Management Supervision
300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
Phone (312) 382-7500
Fax (312) 382-6901

April 5, 2022

Board of Directors
[REDACTED]

Subject: Activity Related to [REDACTED] Bitcoin Service

Dear Board Members:

On December 17, 2021, the Federal Deposit Insurance Corporation (FDIC), the [REDACTED], and [REDACTED] management team participated in a virtual meeting to discuss crypto-asset finder services that [REDACTED] is offering to certain customers. Approximately 2,800 [REDACTED] customers can purchase, sell, and store Bitcoin using an application from [REDACTED] through the bank's online and mobile banking platform provided by [REDACTED]. Subsequent to that meeting, the FDIC and [REDACTED] requested and received additional documentation regarding the bank's agreements, risk assessment, and due diligence related to this new service.

The FDIC has a number of questions based on the information provided to date. Those include questions with respect to the permissibility of this activity, including what legal analysis the bank performed related to permissibility and to assess compliance with Part 362 of the FDIC Rules and Regulations. Those also include questions with respect to safety and soundness¹ related to this activity and consumer protection issues. The FDIC plans to perform a detailed review of this activity and will seek further information with respect to those questions at the upcoming April 25, 2022 joint examination. Until that review is completed, [REDACTED] should not expand the service to additional customers.

If you have any questions, please contact Deputy Regional Director Christopher J. Newbury at [REDACTED].

Sincerely,

GREGORY Digitally signed by
BOTTONE GREGORY BOTTONE
Date: 2022.04.05
12:03:16 -04'00'
Gregory P. Bottone
Regional Director

cc: [REDACTED]

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

DOCUMENT 6



Dallas Regional Office
 600 North Pearl Street, Suite 700
 Dallas, Texas 75201
 (214) 754-0098 FAX (972) 761-2082

April 15, 2022

The Board of Directors
 [REDACTED]
 [REDACTED]
 [REDACTED]

Subject: Proposed New FinTech Product [REDACTED]

Dear Members of the Board:

We received President and Chief Operating Officer [REDACTED] submission on February 23, 2022, that provided high-level information related to the subject [REDACTED] product. The proposed product will apparently be interfaced with the bank's online and mobile banking platforms and will offer bank customers access to Bitcoin and Ethereum through the bank's mobile app. However, at this time the FDIC has not yet determined what, if any, regulatory filings will be necessary for a bank to engage in this type of activity. As a result, we respectfully ask that you pause all crypto asset-related activity. The FDIC will notify all FDIC-supervised banks at a later date when a determination has been made on the supervisory expectations for engaging in crypto asset-related activity, including the need for any regulatory filings. Refer to the Financial Institution Letter issued on April 7, 2022, FIL-16-2022-Notification of Engaging in Crypto-Related Activities, for additional information.

Please direct questions on this matter to Case Manager [REDACTED] at [REDACTED] or [REDACTED]. As a reminder, written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>. If you prefer to send correspondence via mail, please use the Dallas Regional Office address noted in the letterhead. If there are any questions about the Secure Email process, please contact Case Manager [REDACTED].

Sincerely,

Signed by Joseph A. Meade

Joseph A. Meade
 Assistant Regional Director

cc: Federal Reserve Bank of Kansas City
 [REDACTED]

DOCUMENT 7



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 350 5th Avenue, New York, NY 10018

New York Regional Office

April 22, 2022

Board of Directors

[REDACTED]

Subject: Activity Related to [REDACTED]

Dear Members of the Board:

On [REDACTED], the [REDACTED] a [REDACTED] association of [REDACTED] institutions, was launched to further the adoption and interoperability of a [REDACTED] to facilitate the transfer of value on a blockchain. [REDACTED] Bank is currently a member of the [REDACTED]. We appreciate the transparency of [REDACTED] management team over the past several months in keeping us informed as the bank has conducted due diligence and explored its entry into the digital asset space. This letter serves as a follow-up to what was discussed in regards to [REDACTED] activity during the March 25, 2022 call between the [REDACTED] management team and FDIC New York Regional Office staff.

Several key [REDACTED] members participated in a February 22, 2022 conference call to discuss the [REDACTED] and its proposal with representatives from the FDIC, the Board of Governors of the Federal Reserve System, and the Office of Comptroller of the Currency (collectively, Federal regulators). The Federal regulators understand, as a result of this conference call, that the [REDACTED] is currently drafting operating rules to govern transactions on the [REDACTED] blockchain network.

The FDIC has a number of questions based on the information provided to date. We expect the [REDACTED] to address those (in advance of implementation) to ensure member banks are operating in a safe and sound manner.¹ To assist the FDIC and the other Federal regulators in the [REDACTED] review process, we will be sending, under separate cover, (i) the questions regarding the [REDACTED] that have not yet been satisfactorily addressed and (ii) additional questions and document requests that will need to be addressed. In addition to this outreach, we may reach out directly to [REDACTED] with questions to gain an understanding of how the bank will ensure continued safe and sound operation as this activity is implemented.

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

[REDACTED]
Board of Directors

Page 2 of 2

Written correspondence should be addressed to Jessica A. Kaemingk, Acting Regional Director, FDIC, New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (<https://secureemail.fdic.gov/>) using the following email address: NYMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

If you have any questions, please contact Assistant Regional Director Ashley M. Amicangioli at [REDACTED]

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]
Federal Reserve Bank of New York

DOCUMENT 8



Dallas Regional Office
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

April 25, 2022

Board of Directors

[REDACTED]

Via Secure Email

Members of the Board:

On February 22, 2022, the FDIC, OCC, and Federal Reserve Board met with [REDACTED] and banks that were members of [REDACTED] at the time, including [REDACTED] who is a [REDACTED] member of the [REDACTED], General Counsel at [REDACTED], participated in the meeting to discuss the [REDACTED] and its proposed launch. At that meeting, it was evident that the [REDACTED] had yet to finalize the use cases or functionality of the product and the Operating Rules by which the [REDACTED] and its members would be governed. The discussion indicated phases or versions of the product, with future solutions, and subsequently, FDIC has received revised information outlining three models under consideration for the [REDACTED] program.

In our letter to you dated March 11, 2022, the FDIC stated it has a number of questions based on the discussion and information provided to date. The initial questions are attached and we request responses by June 9, 2022. As noted in our prior letter, we expect you to satisfactorily address these and any subsequent questions (in advance of implementation) to ensure the bank is operating in a safe and sound manner.¹ This is consistent with FIL-16-2022 which requests that institutions provide information necessary to allow the agency to assess the safety and soundness, consumer protection, and financial stability implications of such activities.

Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

Kristie Elmquist
Regional Director

Attachment

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations

1. Governance and Structure of [REDACTED].

- a. Describe the activities conducted by [REDACTED]; the assets held by [REDACTED]; the services [REDACTED] provides to [REDACTED] banks; and the relationship between [REDACTED] and [REDACTED] banks.
- b. Describe the governance in place for [REDACTED] private protocol within the [REDACTED] blockchain, including the processes for decision-making, key participants, and key personnel. In your response, indicate the extent to which (i) [REDACTED] will participate in or exercise control over governance of [REDACTED] private protocol within the [REDACTED] blockchain; and (ii) participants on the private protocol could make decisions that would have binding effect with respect to [REDACTED], including over [REDACTED] objections.
- c. Describe what role, if any, [REDACTED] and [REDACTED] will play in the governance of the [REDACTED].
- d. Describe what role, if any, non-member, participating banks will play in the governance of [REDACTED] private protocol, including whether such banks will be restricted in conducting any activities related to the public [REDACTED] blockchain.
- e. Provide the terms of the [REDACTED] smart contract, the rules of the [REDACTED] blockchain and the private protocol, and any documents that describe the terms of such smart contract. Identify the party responsible for creating and coding such terms into the smart contract.
- f. Explain in detail the consensus mechanism for the [REDACTED] blockchain. Identify all persons that control 5 percent or more of the staking assets for the blockchain and provide the percentage controlled.
- g. Explain any dispute resolution processes contemplated with respect to [REDACTED] members.
- h. Provide a list of the fees [REDACTED] has already paid to [REDACTED], and estimated expenses moving forward. In your response, please clarify what the fees are for and whether there are expectations of periodic payments to [REDACTED].
- i. Discuss the permissibility of [REDACTED] membership in [REDACTED] under section 24 of the Federal Deposit Insurance Act, 12 U.S.C. § 1831a, and part 362 of the FDIC Rules and Regulations, 12 C.F.R. part 362.
- j. Clarify whether [REDACTED] operates a node or is otherwise involved in validating transactions on the [REDACTED] blockchain or the private protocol. Identify other entities that operate as a node or otherwise validate transactions. Explain how such nodes are assigned; the role they serve; the governance process for nodes; and whether the nodes for the [REDACTED] private protocol are the same or different than [REDACTED] nodes.
- k. Describe what involvement, if any, [REDACTED] may consider in [REDACTED] related activities of the [REDACTED] blockchain.
- l. Identify the steps that [REDACTED] would need to take if it chooses to exit the [REDACTED].
- m. Describe key third-party relationships that the [REDACTED] and the [REDACTED] will enter into with respect to [REDACTED] activities. In your response, please address any contemplated relationships with [REDACTED] and their affiliates.
- n. If the applications for [REDACTED] include business-to-business payments, merchant payments, and peer-to-peer payments, explain whether different governance protocols would be adopted to ensure privacy, confidentiality and/or data security for the different types of customers and their data.
- o. Explain any restrictions in place regarding the use of data related to [REDACTED] transactions. In your response identify the parties with access to such data and the type(s) of data they

- can access and any controls monitoring the use of such data. Explain the rights and responsibilities with respect to privacy and/or data security violations.
- p. Explain the extent to which [REDACTED] transactions will make use of an off-chain contract execution environment.
 - q. Provide a copy of the Operating Rules.
 - r. Describe any insurance that is contemplated to cover loss or malfeasance at the [REDACTED] or [REDACTED] bank-level.
 - s. Explain whether [REDACTED] banks or participating banks are required to sign exclusivity agreements with the [REDACTED]. In your response, clarify whether [REDACTED] banks or participating banks are allowed to join other similar [REDACTED]
2. **Classifications.**
- a. Explain the difference, if any, between the [REDACTED] use of the terms "[REDACTED]" and "[REDACTED]" (Note these questions use the term "[REDACTED]" but should be read broadly if there is a difference in these terms.)
 - b. The website [REDACTED] (last visited on 3/31/2022) uses the terms "[REDACTED]" and "[REDACTED]". Clarify [REDACTED] understanding of [REDACTED]
 - c. Explain whether the [REDACTED] digital markers identify the issuing bank and how, if at all, this distinction is apparent to banks and/or customers.
 - d. Explain the basis for [REDACTED] determination that its participation in the [REDACTED], including all the activities that it would conduct as part of the [REDACTED] is permissible under applicable law.
3. **Accounting.**
- a. Explain how funds exchanged for [REDACTED] digital markers are reflected on the balance sheet of [REDACTED]
 - b. Explain whether and how the [REDACTED] digital markers themselves are or will be reflected on the balance sheet of [REDACTED]
 - c. Explain whether reserves will be held in connection with the [REDACTED] digital marker liabilities and, if so, whether such reserves be held as cash or in the form of specific assets. If reserves are held, explain whether they serve as collateral for the [REDACTED] digital marker liabilities.
 - d. Provide example general ledger entries for [REDACTED] minting; transfer of [REDACTED] to a customer of another [REDACTED] bank; burning of [REDACTED] and settlement of due-to/due-from balances among [REDACTED] banks. Please provide a chart depicting the flow of funds.
4. **Exposure to Other Members of the [REDACTED].**
- a. Explain how [REDACTED] mitigates the risk of intraday (or over-the-weekend) exposures to other [REDACTED] banks. In your response, describe any controls in place to protect [REDACTED] from the failure of a fellow [REDACTED] bank during the term of these exposures.
 - b. Explain the liability, if any, [REDACTED] would have to holders of [REDACTED] issued by another [REDACTED] bank upon such bank's failure.

5. Risk Management and Controls.

- a. Describe the role of the board in reviewing and approving bank participation in the [REDACTED] and [REDACTED] activities.
 - i. Explain the process by which [REDACTED] board and/or management assessed [REDACTED] authority to participate in the [REDACTED]?
 - ii. Identify the legal risks (including permissibility, if applicable) [REDACTED] board considered when deciding whether to participate in the [REDACTED]. Explain how the [REDACTED] plans to mitigate and manage those risks.
 - iii. If participation in the [REDACTED] was approved by the board, explain the basis upon which the board approved [REDACTED] participation while key questions related to liability, membership, operating rules, and use cases have not been finalized.
 - iv. If participation in the [REDACTED] was not approved by the board, explain management's authority to enter into the activity without board approval.
- b. Explain the type of risk assessment and due diligence that was performed and identify key personnel involved in such activities.
- c. Explain whether management identified relevant expertise needed to engage in this activity.
- d. Explain whether the [REDACTED] established any dollar volume-based limitations on customer activity or bank level activity (on a daily basis) (for example, to monitor total exposure/volume).
- e. Explain whether the bank will upgrade or change any systems or procedures to allow for this activity.
- f. Describe the risk management systems, processes, and controls in place or in development with respect to [REDACTED] activities, including the minting and burning of [REDACTED], maintenance of [REDACTED] wallets, and participation in the [REDACTED] blockchain.
- g. Describe the risk management systems, processes, and controls that [REDACTED] and the [REDACTED] have put in place to monitor and mitigate potential risks posed by the public [REDACTED] blockchain, including those related to blockchain governance disputes, software defects, and changes in protocol rules.
- h. Explain how [REDACTED] public, permissionless nature impacts [REDACTED] ability to mitigate risks related to security and privacy.
- i. Explain how [REDACTED] will mitigate operational risk where a step in the transfer process does not occur as expected.
- j. Provide any continuity plans if the [REDACTED] blockchain fails, including operational errors or delays in processing and system outages.
- k. Describe [REDACTED] efforts to conduct due diligence and assess the risks of engaging in the [REDACTED] smart contract.
- l. Explain how [REDACTED] will ensure that the amount of funds in the omnibus deposit account matches, at a minimum, at all times the aggregate amount of [REDACTED] in its customers' wallets.
- m. Describe any testing [REDACTED] is conducting or will conduct in relation to the [REDACTED] blockchain, [REDACTED] smart contract, or other aspects of its participation in the [REDACTED].
- n. Describe and provide documentation of vulnerability analysis that has been performed related to the smart contracts.

6. **Settlement:** Explain when the final settlement of a transaction facilitated by [REDACTED] occurs, where it is recorded, and whether there are any dependencies on the public [REDACTED] blockchain for settlement finality.
- Provide a detailed account of what "[REDACTED]" is and for what it will be used. In your response, include whether it has a set price or whether its price can fluctuate.
 - Explain whether [REDACTED] will be paying "[REDACTED]" fees directly to update the [REDACTED] blockchain ledger and, if so, to whom such fees are paid.
 - Explain whether [REDACTED] plans to hold "[REDACTED]" and, if so, (i) how it will be reflected on [REDACTED] balance sheet and (ii) how much the [REDACTED] plans to hold. If its price can fluctuate, explain how [REDACTED] intends to account for variations in the price of "[REDACTED]"
 - Provide a description of the accounting methods and treatment used for [REDACTED] held by [REDACTED] (including initial recording and any subsequent entries).
7. **Use Cases**
- Provide a detailed description of planned and potential use cases for [REDACTED]
 - Explain how the [REDACTED] differs from other bank-offered peer-to-peer payments platforms (e.g., [REDACTED]). Explain if the [REDACTED] interacts with any such platforms.
 - Explain whether and how the [REDACTED] is developing an alias directory (e.g. email addresses). If so, explain (i) whether such directory will be housed by a central party, or such data will be stored in a decentralized manner; how any personal identifiable information (PII) stored in the alias directory will be protected.
 - Explain how customers effectuate peer-to-peer payments (e.g., in banks' own apps or via a third-party app).
 - Identify and describe safeguards that will be put in place to mitigate the risk that customers send funds to an unintended recipient.
 - Provide screen shots to show the customer's user experience.
8. **Consumer Protection.**
- Identify the fees and other charges that will be imposed on [REDACTED] customers that elect to use [REDACTED] to conduct transactions.
 - Describe the anticipated process for managing complaints from [REDACTED] customers related to [REDACTED].
 - Explain any steps [REDACTED] will take to ensure consumers understand any difference in protections between [REDACTED] and traditional banking products.
 - Describe network rules, systems, and practices that will be put in place to protect consumers. For example, explain the rights consumers will have to dispute errors, payments mistakenly sent to the wrong party, or payments related to fraud. Describe how [REDACTED] and the [REDACTED] will ensure such disputes are resolved in a timely basis and in accordance with network rules and applicable laws and regulations.
 - Explain whether [REDACTED] or any other entity will indemnify customers for breaches to the wallets.
 - Explain whether consumers are required to enter into an agreement with [REDACTED] (or another entity) to maintain a wallet.
 - Describe any representations that [REDACTED] is making or plans to make regarding the applicability of FDIC deposit insurance.

- h. Describe any representations that [REDACTED] is making or plans to make regarding the stability of [REDACTED], including regarding reserves.
- i. Explain whether responsibility for approval of advertising and marketing materials rests with individual [REDACTED] banks or the [REDACTED] as a whole, or if there is some other arrangement.
- j. Identify the consumer data that will be shared with the [REDACTED] and its participants, as well as any controls in place to protect PII and limit sharing. In your response, indicate whether any PII will be stored on a distributed ledger and describe any disclosures regarding data sharing that [REDACTED] intends to provide.

DOCUMENT 9



Dallas Regional Office
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

SENT VIA SECURED ELECTRONIC MAIL

May 4, 2022

The Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Proposed Crypto Asset Capability

Dear Members of the Board:

This office received Senior Vice President and Compliance Officer [REDACTED] e-mail sent on April 19, 2022, that provided high-level information about the bank's intent to provide a crypto asset capability involving [REDACTED]. The relationship with [REDACTED] would provide bank customers an avenue to engage in crypto asset transactions, specifically the purchase and sale of Bitcoin, using the bank's mobile banking application. We thank you for your timely notification as requested by Financial Institution Letter (FIL-16-2022) dated April 7, 2022.

At this time the FDIC has not yet determined what, if any, regulatory filings will be necessary for a bank to engage in this type of activity. As a result, we respectfully ask that you not implement this product, while we consider this crypto asset-related activity.

As we review your proposed activity, we will continue to correspond with your institution regarding additional information requests to aid us in our assessment of the activity. In the meantime, you may direct questions on this matter to Case Manager [REDACTED] at [REDACTED]. Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

/s/ J. Mark Love

J. Mark Love
Assistant Regional Director

cc: Federal Reserve Bank of Dallas
[REDACTED]

DOCUMENT 10



Dallas Regional Office
 600 North Pearl Street, Suite 700
 Dallas, Texas 75201
 (214) 754-0098 FAX (972) 761-2082

May 13, 2022

Board of Directors

[REDACTED]
 [REDACTED]
 [REDACTED]

Subject: Third-Party Bitcoin Facilitation Activity

Dear Members of the Board:

By letter dated December 30, 2021, [REDACTED] President of [REDACTED] (the Bank), advised the FDIC and the [REDACTED] of the Bank's intent to offer Bank customers the ability to buy, hold, and sell bitcoin through the Bank's online banking website and mobile application in conjunction with [REDACTED] (bitcoin trading platform) and [REDACTED] (technology provider). The relationship allows Bank customers to purchase and sell bitcoin through [REDACTED], with funds flowing through the customer's account at the Bank.

By letter dated January 19, 2022, additional information was received from President [REDACTED] regarding this service, and a brief conference call with President [REDACTED], the [REDACTED], and a representative from the FDIC was held on January 26, 2022. By letter dated February 9, 2022, the FDIC and [REDACTED] outlined certain information included in the November 23, 2021 Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (Joint Statement).

On April 7, 2022, the FDIC issued a Financial Institution Letter, FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. That FIL is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

On April 14, 2022, President [REDACTED] verbally notified Case Manager [REDACTED] that the Bank had launched the bitcoin facilitation activity on [REDACTED]. To date, approximately 36 number of customers have executed transactions, with most transactions being bitcoin purchases.

The FDIC continues to review the bitcoin facilitation activity and various questions remain outstanding, including with respect to the legal permissibility of this activity, the potential applicability of part 362 of the FDIC Rules and Regulations, and safety and soundness and consumer protection principles. Consistent with the procedures outlined in FIL-16-2022, the FDIC will make future information requests to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service to additional customers.

Page 2

Sincerely,

CC: [REDACTED]

DOCUMENT 11

**Federal Deposit Insurance Corporation**

Division of Risk Management Supervision and Division of Depositor and Consumer Protection
350 5th Avenue, New York, NY 10018

New York Regional Office

June 22, 2022

Board of Directors
[REDACTED]

Subject: [REDACTED] Notice to Engage in Digital Asset Activities under FIL-16-2022

Dear Members of the Board:

We received the subject correspondence dated May 20, 2022 from [REDACTED] (Bank), in response to Financial Institution Letter 16-2022, notifying the FDIC of the Bank's intent to engage in activities involving digital assets. New York Regional Office staff has met numerous times with Bank management over the past several months regarding these proposed activities. We appreciate management's efforts to keep us informed as the Bank has conducted due diligence and explored its entry into the digital asset space.

The FDIC has a number of questions regarding the activities based on the information provided to date. The FDIC plans to conduct a targeted review of the Bank's planned digital asset activities in July 2022 to gain an understanding of how the Bank will ensure continued safe and sound operations and consumer protections, should these activities be implemented. A document request list related to this targeted review was provided under separate cover. The Bank should address these questions, in advance of implementation of the proposed activities, in order for the FDIC to assess the safety and soundness of the proposed activities¹ and compliance with laws and regulations.

If you have any questions, please contact Assistant Regional Director Ashley M. Amicangioli at [REDACTED] or Assistant Regional Director Kara L. Ritchie at [REDACTED].

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

CC: [REDACTED]

¹ See e.g., Section 39 of the Federal Deposit Insurance Act and Part 364 of the FDIC Rules and Regulations.

DOCUMENT 12



Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
Phone (312) 382-7500
Fax (312) 382-6901

June 27, 2022

Board of Directors
[REDACTED]

Subject: Third-Party Bitcoin Facilitation Activity

Dear Members of the Board:

By letter dated May 27, 2022, [REDACTED] Vice President/Compliance Officer of [REDACTED] (the Bank), advised the FDIC, in response to Financial Institution Letter 16-2022 (FIL-16-2022),¹ and the [REDACTED] of the Bank's intent to offer Bank customers the ability to buy, hold, and sell bitcoin through the Bank's online banking website and mobile application in conjunction with [REDACTED] and certain of its subsidiaries (collectively, [REDACTED] and [REDACTED] (technology provider). The relationship allows Bank customers to purchase and sell bitcoin through [REDACTED], with funds flowing through the customer's account at the Bank, as facilitated by the technology provider.

On June 14, 2022, Vice President/Compliance Officer [REDACTED] verbally informed Acting Case Manager [REDACTED] that the Bank would begin marketing the bitcoin facilitation activity to Bank customers on [REDACTED]. To date, the Bank has enrolled 20 customers, all employees of the bank, with transactions totaling approximately \$1,400.

The FDIC continues to review the bitcoin facilitation activity and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC will request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service.

If you have any questions, please contact Acting Case Manager [REDACTED] at [REDACTED] or Review Examiner [REDACTED] at [REDACTED]. Written correspondence should be addressed to my attention at the Chicago Regional Office, and sent as a PDF document through [REDACTED].

¹ On April 7, 2022, the FDIC issued FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. FIL-16-2022 is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address:
CHIMailRoom@FDIC.gov.

Sincerely,

Gregory P. Bottone
Regional Director

cc: [REDACTED]

DOCUMENT 13



Federal Deposit Insurance Corporation
350 Fifth Avenue, Suite 1200, New York, NY 10118

New York Regional Office

June 30, 2022

Board of Directors

Subject: Third-Party Bitcoin Facilitation Activity

Dear Members of the Board:

In a December 13, 2021 meeting, [REDACTED] (Bank) officers¹ advised the FDIC of the Bank's intent to offer customers the ability to buy, hold, and sell bitcoin through the online banking website and mobile application in conjunction with [REDACTED] and [REDACTED]. The relationship allows Bank customers to purchase and sell bitcoin through [REDACTED], with funds flowing through the customer's account at the Bank.

In a letter dated May 19, 2022, EVP Chief Digital Payments Officer [REDACTED] provided an overview of the program and due diligence activities in response to the FDIC Financial Institution Letter, FIL-16-2022, dated April 7, 2022 (FIL-16-2022). FIL-16-2022 explains the notification and supervisory feedback process concerning current or planned crypto-asset-related activity. On June 1, 2022, the Bank, the FDIC, and [REDACTED] discussed the program again. The program was rolled out to a select group of employees or [REDACTED].

The FDIC continues to review the bitcoin activity and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC will request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the bank refrain from expanding this service.

If you have any questions, please contact Assistant Regional Director Catherine H. Goni at [REDACTED]. Written correspondence should be addressed to my attention at the New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail@fdic.gov) using the following e-mail address: NYMailroom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,
Jessica A. Kaemingk
Acting Regional Director

cc: [REDACTED]

¹ Chief Risk Officer [REDACTED], Chief Information Officer [REDACTED], Executive Vice President Chief Digital Payments Officer [REDACTED], and Vice President Compliance Officer [REDACTED]

DOCUMENT 14



Division of Risk Management Supervision
Division of Depositor and Consumer Protection

Dallas Regional Office
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

July 14, 2022

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Third-Party Bitcoin Activity

Dear Members of the Board:

By letter dated July 8, 2022, [REDACTED] (Bank) provided notification pursuant to Financial Institution Letter-16-2022, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022), of its program offering customers the ability to buy, hold, and sell bitcoin through the Bank's online banking website in conjunction with [REDACTED]. This relationship allows Bank customers to purchase and sell bitcoin through [REDACTED], with funds flowing through the customer's account at the Bank.

On June 21, 2022, the FDIC held a videoconference meeting, with members of the Bank's executive team to discuss the bitcoin activity. Chief Executive Officer (CEO) [REDACTED], President [REDACTED], General Counsel [REDACTED], and Compliance Officer (CO) [REDACTED] represented the Bank. Assistant Regional Director (ARD) J. Mark Love, ARD Cynthia Scott, ARD Akhtar Khan, and Case Manager [REDACTED] represented the FDIC.

During the meeting, GC [REDACTED] informed the FDIC that the program is live as of [REDACTED], the Bank does not directly engage in bitcoin activity on behalf of customers, and the activities are transacted on a platform provided by [REDACTED] that is integrated into the Bank's online banking website by a technology service provider. GC [REDACTED] committed to provide additional information about the activity, including screenshots of the customer-facing disclosures, a risk assessment of the activity, and the vendor management due diligence of [REDACTED]. In addition, GC [REDACTED] committed to provide, by July 8, 2022, user data, including the number of current users, the number of active users, the number of transactions, and the average and total dollar amount of transactions related to the activity. Subsequent to this meeting, the Bank advised the FDIC that 70 Bank customers have established accounts, 30 of which have conducted at least one transaction. The Bank stated that the total transaction volume since inception is \$35,906, with an average balance held in each account of \$2,933.

The FDIC continues to review crypto-related activities and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC may request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service.

If you have any questions, please contact ARD Love at [REDACTED]. Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

[REDACTED]
Third-Party Bitcoin Activity

Page 2

Sincerely,

/s/ Kristie K. Elmquist

Kristie K. Elmquist
Regional Director

cc: [REDACTED]

DOCUMENT 15

**FDIC**

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

Division of Risk Management Supervision
San Francisco Regional Office
(415) 546-0160

July 27, 2022

Board of Directors
[REDACTED]
[REDACTED]

Subject: Notification of Crypto-Related Activity

Dear Members of the Board:

By letter dated March 22, 2022, [REDACTED], SVP/CRO of [REDACTED], (the Bank) notified the FDIC and the [REDACTED] that the Bank will provide its customers the ability to buy, sell, and hold bitcoin through the Bank's online banking website in conjunction with [REDACTED] and [REDACTED]. The relationship will allow Bank customers to purchase, hold, and sell bitcoin through [REDACTED], with funds flowing through the customer's account at the Bank. [REDACTED] will maintain custody of the bitcoin accounts.

On April 7, 2022, the FDIC issued a Financial Institution Letter, FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. That FIL is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

By email dated May 4, 2022, SVP/CRO [REDACTED] provided the FDIC and [REDACTED] with due diligence documents related to the bitcoin activities as attachments to the email. These documents include the following: [REDACTED]
[REDACTED]
[REDACTED]

On May 31, 2022, a joint FDIC and [REDACTED] Safety and Soundness examination began. On June 15, 2022, examiners and bank management held an MS Teams Meeting to present an additional request list related to the proposed crypto activities. During the meeting, a live demonstration of the Bank's test environment was held whereby a bank employee bought and sold bitcoin. Bank management noted that the ability to buy/sell/hold bitcoin is currently limited to a test environment, and only certain employees have access to the test environment.

The FDIC continues to review the bitcoin activities and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC has requested information as part of the examination process and may request additional information to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service to its customers.

If you have any questions, please contact RMS Assistant Regional Director David Wong at [REDACTED] or DCP Assistant Regional Director Matthew Sheeren 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 about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,

Digitally signed by
KATHY MOE
Date: 2022.01.27
15:37:43 -0700
Kathy L. Moe
Regional Director

[REDACTED]

DOCUMENT 16

**FDIC**

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

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

Sent via secure email to [REDACTED]

July 28, 2022

Board of Directors
[REDACTED]

Subject: Notification of Engaging in Crypto-Related Activities

Dear Members of the Board:

On May 31, 2022, [REDACTED] Chief Financial Officer (CFO) [REDACTED] submitted [REDACTED] draft three-year business plan (Plan) pursuant to FDIC's Financial Institution Letter-16-2022, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022). We also held a brief discussion with President and Chief Executive Officer [REDACTED], CFO [REDACTED] and the Digital Banking Division's Chief Operating Officer [REDACTED] on June 22, 2022. As discussed during the call, the Plan represents a significant and material change in the bank's business model as it seeks to develop and implement a proposed Digital Banking Platform (DBP) strategy.

While the FDIC continues to review the bank's Plan pursuant to FIL-16-2022, in order to assess the safety and soundness and consumer protection implications of such activities, additional information is needed and questions remain outstanding. We recognize that the Plan is early in its implementation stages, and that developing the risk management framework is an ongoing process; however, it is essential for management to solidify this framework prior to implementation to ensure planned activities and strategies are consistent with current laws, rules, and regulations, as well as safety and soundness and consumer protection principles. Examples of incomplete, but essential, elements that we request the opportunity to review, when available, include the following:

- Risk assessments for DBP activities,
- Due diligence for all vendors related to the Digital Banking Division, as well as the identification of vendors to assist in customer due diligence, custodial services, exchange services, funds movement, and any other services related to DPB,
- Policies and procedures and planned products and services surrounding the Digital Banking Division,
- Project plans and cost benefit analysis for DBP activities,
- Formal succession plan for the Digital Banking Division,

Board of Directors

██████████
Page 2

- Draft contracts and legal agreements between the bank and its affiliate entities, as well as key third parties,
- Legal analysis of the permissibility of the proposed new products and services under Part 362 of the FDIC's Rules and Regulations, including the permissibility of BTC/ETH as collateral and the applicability of 12 C.F.R. § 1.7 with respect to the Digital Assets Lending Program,
- Also with respect to the Digital Assets Lending Program:
 - Identification of loan types, policies, target loan mix, and anticipated direct and indirect loan relationships,
 - Legal analysis of: (1) how ██████████ would perfect its security interest in BTC/ETH collateral under the ██████████ Uniform Commercial Code (UCC), (2) the priority of ██████████ security interest in BTC/ETH collateral under the ██████████ UCC, (3) how ██████████ would foreclose on BTC/ETH under ██████████ law, and (4) the applicability of Regulation U (12 C.F.R. Part 221) to the proposed program.
- Banking services to be offered to fintech platforms and ecosystem participants,
- Plans to expand the bank's lending outside of its existing assessment area or market area as a result of the DBP strategy, if any, and expected impacts to the Community Reinvestment Act (CRA) performance,
- Any assessment of consumer protection risk considerations; for example, any potential consumer harm or consumer confusion associated with planned products and services offered by the Digital Banking Division,
- Analysis performed with respect to SEC Staff Accounting Bulletin No. 121 and proposed new products and services, and,
- Plans for ongoing monitoring and audit of the Digital Banking Platform.

As noted throughout the Plan and during our discussion, we understand that much of the development, acquisition, and pursuit of the various DBP strategies remain in process. As a result, we expect to remain in close correspondence with the bank in the coming weeks and months. Also, please note that FIL-16-2022 does not provide for the issuance of an FDIC non-objection, as requested in the Plan. Consistent with the procedures outlined in FIL-16-2022, the FDIC may make future information requests to assist us in reviewing the activities and providing any relevant supervisory feedback to the bank. Accordingly, until we complete our review, we request that the bank not proceed with planned activities, pending FDIC supervisory feedback, and that you continue to update us on developments in the bank's risk management framework and compliance management system.

If you have any questions related to Risk Management, please contact Assistant Regional Director Jaclyn Valderrama or Case Manager ██████████ at ██████████ and ██████████, respectively. For questions related to Consumer Protection, please contact Assistant Regional Director Matthew Sheeren or Review Examiner ██████████ at ██████████ and ██████████, respectively. 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

Board of Directors
[REDACTED]

Page 3

portal (<https://securemail.fdic.gov/>) using the following e-mail address: SFMailRoom@fdic.gov. Information about 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

cc:

[REDACTED]
Federal Reserve Bank of San Francisco

DOCUMENT 17



Federal Deposit Insurance Corporation
1100 Walnut Street, Suite 2100, Kansas City, MO 64106

Division of Risk Management Supervision

August 9, 2022

Board of Directors
[REDACTED]

Subject: Third-Party Bitcoin Facilitation Activity

Dear Members of the Board:

By letter dated May 10, 2022, [REDACTED], President and CEO of [REDACTED] (Bank), advised the FDIC of the bank's intent to offer customers the ability to buy, sell, and hold bitcoin through the Bank's digital and mobile banking platform in conjunction with [REDACTED] (bitcoin facilitation activity) in response to FIL-16-2022.¹ The relationship allows Bank customers to purchase and sell bitcoin with [REDACTED] as the trade execution provider and custodian and with all customer orders and transaction confirmations flowing through the Bank (bitcoin trading platform). The Bank also plans to offer a debit card with cash rewards that [REDACTED] pays in the form of bitcoin. Furthermore, [REDACTED] advised that credit was extended in November 2021 to [REDACTED], in the amount of \$[REDACTED]. The credit is secured by bitcoin and contains a 50 percent margin requirement, updated daily.

On March 11, 2022, the Bank discussed the bitcoin facilitation activity with the FDIC Division of Depositor and Consumer Protection – Kansas City Regional Office (RO). Follow-up discussions were held on April 12, 2022, and June 2, 2022. During the course of those discussions Bank management explained that beta testing of the bitcoin trading platform had commenced, with plans to expand that beta testing to non-customers. By letter dated June 3, 2022, additional information from the Bank was forwarded to the RO documenting the Bank's due diligence regarding the bitcoin facilitation activity and the loan presentation for the credit extended to [REDACTED] in November 2021.

The FDIC continues to review the bitcoin facilitation activity and various questions remain outstanding. Consistent with the procedures outlined in FIL-16-2022, the FDIC will make future information requests to assist us in reviewing the activity and providing supervisory feedback to the Bank. Accordingly, until we complete our review, we request that the Bank refrain from expanding this service to additional customers.

¹ On April 7, 2022, the FDIC issued a Financial Institution Letter, FIL-16-2022, explaining a notification and supervisory feedback process concerning a bank's current or planned crypto-asset related activity. That FIL is available here: <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>.

Case 1:24-cv-01857-ACR Document 27-2 Filed 01/17/25 Page 51 of 80

If you have any questions, please contact Assistant Regional Director Michele Sharp or Case Manager [REDACTED] at [REDACTED]. Written correspondence should be addressed to my attention at the Kansas City 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: KCMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

Sincerely,
James D. LaPierre
Regional Director

cc: [REDACTED]

DOCUMENT 18



FEDERAL DEPOSIT INSURANCE CORPORATION
10 10th Street NE, Suite 800
Atlanta, Georgia 30309-3849

Atlanta Regional Office
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
(678) 916-2200

August 26, 2022

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Notification of Crypto-Related Activity

Dear Members of the Board:

On August 5, 2022, the FDIC received [REDACTED] (Bank) notification, in response to Financial Institution Letter (FIL), FIL-16-2022, Notification of Engaging in Crypto-Related Activities, of the Bank's intent to engage in crypto-asset related activity by offering customers bitcoin services through the Bank's banking platform in conjunction with [REDACTED]. 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 Bank's notification outlines that crypto-asset related activity includes offering customers the ability to buy, hold, and sell bitcoin ([REDACTED] Platform); a [REDACTED] Program; and a [REDACTED] Program.

The letter states that the Bank intends to start offering these services to customers on [REDACTED]. 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 such activities. To assess these risks, the FDIC is reviewing the notification and information provided, and is also assessing whether the proposed crypto-asset activities constitute a major deviation or material change in the business plan that the Bank must operate within during its [REDACTED] under the Deposit Insurance Order dated [REDACTED].

To assist in our review of the proposed activities, please provide the documentation referenced in the Appendix attached to this letter. We will review this documentation to assess the safety and soundness, consumer protection, and financial stability implications of such activities as it is received and in conjunction with the safety and soundness examination scheduled to commence on September 26, 2022. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the Bank refrain from providing this service to its customers.

Please submit the information requested in the Appendix to the FDIC as a PDF file to ATLMailRoom@fdic.gov using the secure message center at <https://securemail.fdic.gov>. The

information should be submitted to this office by September 9, 2022. If you foresee any issues with meeting this deadline, please contact the individuals identified below.

If you have any questions related to Risk Management, please contact Case Manager [REDACTED] at [REDACTED] or at [REDACTED]. If you have any questions related to Consumer Protection, please contact Senior Review Examiner [REDACTED] at [REDACTED] or at [REDACTED].

Sincerely,

Frank R. Hughes
Acting Regional Director

cc: [REDACTED]

Appendix
Crypto-Related Activity Request List

Please provide the following documentation in relation to the proposed crypto-related activities:

1. All contracts (including any draft contracts that the 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 for each activity (i.e., [REDACTED] Platform, [REDACTED] Program, and [REDACTED] Program);
5. Detailed description of the settlement process for customer buy/sell transactions between the Bank [REDACTED], and any other related parties for each activity (i.e., [REDACTED] Platform, [REDACTED] Program, and [REDACTED] Program);
6. The Bank's permissibility analysis and determination with respect to each activity;
7. The Bank's analysis of SEC SAB 121 and its applicability;
8. Any cost-benefit analysis conducted;
9. Project plan for each activity;
10. Vendor management due diligence analysis related to [REDACTED] and vendor due diligence documentation and analysis related to [REDACTED] role in this product (including audits, financials, insurance, complaints, etc.);
11. Description of what happens to customers' accounts or holdings of Bitcoin if the Bank does not continue or cancels offering the services provided by [REDACTED];
12. Details on operational aspects of the [REDACTED] and [REDACTED] Programs including, but not limited to: 1) the types of credit and debit cards or savings and money market accounts that can be enrolled in the program, 2) the process of converting [REDACTED] or USD to Bitcoin, 3) when and how transaction receipts are provided for purchase transactions, 4) and if and how customers can turn the features on or off for any given period;
13. Description of any fees charged to consumers related to the [REDACTED] Platform, [REDACTED] Program, and [REDACTED] Program, and how they will be calculated (describe if and how fees are split amongst the Bank and any third parties involved in the activities);
14. Description of any transaction limitations imposed by [REDACTED] or the Bank on the amount of Bitcoin a consumer may purchase or sell through the [REDACTED] Platform (e.g., daily, weekly, monthly). Similarly, describe any transaction limitations that exist, if any, through the [REDACTED] Program and [REDACTED] Program (including any minimum purchase amounts). Provide a description of the methodology that determines the price a consumer pays to [REDACTED] for Bitcoin through the [REDACTED] Platform, [REDACTED] Program, and [REDACTED] Program. This includes providing an explanation of how any market or benchmark price is determined and how the spread, if any, is calculated;
15. Copies of consumer agreements, disclosures, and other terms and conditions related to each of the activities provided by or through the Bank and by third parties (draft or proposed);
16. Marketing materials, press releases, internal scripts, educational materials, and any other publicly distributed information related to each of the activities (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 consumers by, or through, the Bank in connection with each of the activities;

17. Strategic plan that details how crypto-asset activities achieve the objectives of the Board and any contingency plan, should the activities fail to achieve the objectives;
18. Implementation plan. For each activity, please include expected volumes, income projections used to determine whether the products are financially feasible, and any other analysis performed to support launching the products;
19. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activities;
20. Internal training materials related to the activities;
21. Policies and procedures that will govern each of the crypto-related activities, including those related to consumer compliance and complaint resolution (we acknowledge receipt of the policy outline previously submitted, this request is for the policies and procedures);
22. 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); and
23. Description addressing the following: when a customer enrolls in the [REDACTED] Platform, [REDACTED] Program, and [REDACTED] Program, are the individual customer's Bitcoin balances purchased through each feature presented in aggregate or by program within the online banking and mobile application interface.
24. Describe how the risk assessment was developed, what policies govern the structure/process for risk assessments, and which staff performed the risk assessment. Explain how the Bank determined the risk assessment scope is appropriate for all three product types collectively [REDACTED], [REDACTED], and [REDACTED].
25. The Risk Assessment includes the following statement under [REDACTED],
 "[REDACTED]
 [REDACTED]"
 - a. Provide any quantitative analysis including projections and stress events developed by the Bank to support this [REDACTED].
26. The Risk Assessment includes the following statement, "[REDACTED]"
 - a. Provide the Bank's legal analysis and support for that statement.
27. The Risk Assessment includes the following statement under Compliance Risk, "[REDACTED]"
 - a. Provide the relevant audit reports that the Bank considers as the risk mitigants.
28. The Risk Assessment includes the following statement under Compliance Risk, "[REDACTED]"
 - a. Provide a description of PII exchanged between the bank, the technology service provider, and [REDACTED].
29. The Risk Assessment includes the following statement under Operational Risk, "[REDACTED]"
 - a. Provide a copy of these reports.
30. The Risk Assessment includes the following statement under Operational Risk, "[REDACTED]"
 - a. Provide a copy of the general and digital asset-specific insurance policies.

31. The Risk Assessment includes the following statement under Operational Risk, "[REDACTED]"
- a. Provide a copy of the [REDACTED] the bank has considered as operational risk mitigants.
32. The Risk Assessment includes the following statement under Reputational Risk, "[REDACTED]"
- a. Provide a copy of analysis performed regarding this stated "[REDACTED]"
33. Page 15 of the Risk Assessment includes the following statement, "[REDACTED]"
- [REDACTED]
- [REDACTED]
- a. Provide information regarding these controls, protocols, and systems developed and implemented by the Bank.
34. Page 17 of the Risk Assessment includes the following statement, "[REDACTED]"
- a. Explain how the Bank performs this monitoring and provide copies of monitoring reports.
35. Page 17 of the Risk Assessment also includes the following statement, "[REDACTED]"
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- a. Explain how management assessed the adequacy of the Bank's management information systems relative to this service.
- b. Provide a description of the controls that have been established as stated.
- c. Provide copies of the described monitoring, reporting, and exception management documentation.
36. Page 18 of the Risk Assessment also includes the following statement, "[REDACTED]"
- [REDACTED]
- a. Provide any such reports or anticipated content of such reports planned for Audit Committee.

DOCUMENT 19



Federal Deposit Insurance Corporation
 Division of Risk Management Supervision
 Division of Depositor and Consumer Protection
 300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
 Phone (312) 382-7500
 Fax (312) 382-6901

September 9, 2022

Board of Directors
 [REDACTED]

Subject: Third-Party Crypto-Asset Activity

Dear Members of the Board:

On June 30, 2022, Executive Vice President [REDACTED] submitted a notification of the Bank's intended crypto-asset activities in response to Financial Institution Letter-16-2022, *Notification of Engaging in Crypto-Related Activities* (FIL-16-2022). Acting Case Manager [REDACTED] also held a discussion with Head of Digital Assets [REDACTED] on July 15, 2022 regarding the proposed crypto-asset activities. As discussed during the call, [REDACTED] is developing a Digital Asset department and seeks to implement the following crypto-asset services for bank customers: custodian services (end of the third quarter 2022); facilitation of buying and selling crypto-assets (after custodian services implementation); and, allowing customers to spend/withdraw bitcoin (no timeline).

The FDIC requests insured depository institutions provide sufficient information to assist the FDIC to assess the safety and soundness, consumer protection, and financial stability implications of crypto-asset activities. The FDIC requests the Bank provide the information in the attached list by October 18, 2022, so that the FDIC may begin those assessments. If the requested information has not yet been developed, provide the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the requested information, we will determine whether additional information is necessary to complete the review of the activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the Bank not proceed with planned activities, pending FDIC supervisory feedback.

If you have any questions, please contact Case Manager [REDACTED] at [REDACTED] or Regional Examination Specialist [REDACTED] at [REDACTED]. Written correspondence should be addressed to my attention at the Chicago Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: CHIMailRoom@FDIC.gov.

Sincerely,
 Gregory P. Bottone
 Regional Director

Enclosure – Crypto-Asset Activity Request List

cc: [REDACTED]
 Federal Reserve Bank of Chicago

Crypto-Asset Activity Request List

1. Strategic Plan that details how crypto-related activity achieves objectives of the Bank's Board and the Contingency Plan in the event the activity fails to achieve those objectives.
2. Project/Implementation plan including, but not limited to, expected volumes of activity or contemplated activity limits, cost benefit analysis including income projections used to determine whether the services are financially feasible, and any other analysis performed to support launching the services.
3. Risk assessments for all crypto-related services. Consideration should be made to Safety and Soundness, Information Technology, Anti-Money Laundering/Combating the Financing of Terrorism, and Consumer Compliance.
4. Vendor management due diligence documentation, and analysis for all vendors that will provide crypto-related technologies or services.
5. Board and committee minutes reflecting approval, discussion, analysis, and any documentation provided on the activity.
6. Draft contracts and legal agreements between the Bank and crypto-related third party vendors.
7. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution.
8. If not outlined in policies and procedures, the framework of assigned responsibilities and qualifications for those involved in day-to-day administration of digital asset activity, including internal controls responsibilities, and a description of oversight responsibilities, for example: management; staff; committees, including committee members; frequency of meetings; and collectively, their approval authority, and expertise required to be a committee member.
9. Draft marketing plans, including press releases, educational and training materials, and any other proposed public distributions.
10. Draft consumer agreements, disclosures, or other terms and conditions related to these activities provided by, or through, the Bank and by third parties.
11. Legal analysis of the permissibility of the proposed services under part 362 of the FDIC's Rules and Regulations, and under the State of [REDACTED] banking regulations.
12. Analysis performed with respect to SEC Staff Accounting Bulletin No. 121 and proposed services.
13. Plans for ongoing monitoring and audit of crypto-related products and services.

DOCUMENT 20



FEDERAL DEPOSIT INSURANCE CORPORATION
10 10th Street NE, Suite 800
Atlanta, Georgia 30309-3849

Atlanta Regional Office
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
(678) 916-2200

September 13, 2022

Sent via secure email

Board of Directors
[REDACTED]
[REDACTED]
[REDACTED]

Subject: Third-Party Crypto-Asset Activity

Dear Members of the Board:

On August 17, 2022, we received [REDACTED] (the Bank) notification, in response to Financial Institution Letter (FIL), [FIL-16-2022, Notification of Engaging in Crypto-Related Activities](#), of the Bank's intent to offer customers the ability to buy, sell, and hold Bitcoin through the Bank's digital and mobile banking platform in conjunction with [REDACTED]. 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") promptly notify the appropriate FDIC Regional Director.

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 such activities. In order to begin those assessments, please provide the information in the attached list by November 14, 2022. If the requested information has not yet been developed, include the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the above-requested information, we will determine whether additional information is necessary to complete the review of the activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the Bank refrain from providing these services to its customers.

Board of Directors
[REDACTED]

Page 2 of 2

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 [REDACTED] at [REDACTED] or [REDACTED] or Review Examiner [REDACTED] at [REDACTED] or [REDACTED]. Written correspondence should be addressed to my attention at the Atlanta Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using the following e-mail address: ATLMailRoom@fdic.gov.

Sincerely,

JOHN

Digitally signed
by JOHN VOGEL
Date: 2022.09.13
16:45:08 -04'00'John F. Vogel
Acting Regional Director

cc: [REDACTED]

Enclosure

Crypto-Asset Activity Request List

Documentation (Prospective):

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. The bank's permissibility analysis and determination with respect to the activity
5. Bank's analysis of SEC SAB 121 and its applicability
6. Cost-benefit analysis
7. Project plan
8. Vendor management due diligence documentation and analysis related to both [REDACTED] and [REDACTED] including audits, financials, insurance, complaints, etc.
9. Description of what happens to customers' accounts or holdings of Bitcoin if the bank does not continue or cancels offering the services provided by [REDACTED]
10. Description of any fees that will be charged to consumers related to the activity, and how they will be calculated. Also, describe if and how fees are split amongst the bank and any third parties involved in the activity.
11. Description of any transaction limitations imposed by [REDACTED] or the bank on the amount of Bitcoin a consumer may purchase or sell (e.g. daily, weekly, monthly).
12. Description of the methodology that determines the price a consumer pays to [REDACTED] for Bitcoin. This includes providing an explanation of how any market price is determined and how the spread, if any, is calculated.
13. Consumer agreements, disclosures, and other terms and conditions related to the activities provided by or through the bank and by third parties (draft or proposed)
14. 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 consumers by, or through, the bank in connection with activities.
15. Any other due diligence materials.
16. Strategic plan that details how crypto-asset activity achieves objectives of the board and the contingency plan should the activity fail to achieve the objectives.
17. 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.
18. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activity.
19. Risk assessment(s) related to the activity.
20. Internal training materials related to the activity.
21. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution.
22. 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).

DOCUMENT 21



FEDERAL DEPOSIT INSURANCE CORPORATION
600 North Pearl Street, Suite 700
Dallas, Texas 75201
(214) 754-0098 FAX (972) 761-2082

Dallas Regional Office
Division of Risk Management Supervision
Division of Depositor and Consumer Protection

SENT VIA SECURE ELECTRONIC EMAIL

September 14, 2022

Board of Directors
[REDACTED]

Subject: Notification of Crypto-Asset Related Activity

Dear Members of the Board:

By email dated August 17, 2022, Senior Vice President/Chief Operating Officer [REDACTED] notified us of [REDACTED] intent to provide its customers the ability to buy, sell, and hold Bitcoin through a mobile banking platform in conjunction with [REDACTED]
[REDACTED]

As stated in FIL-16-2022, *Notification of Engaging in Crypto-Related Activities*, 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 such activities. In order to begin those assessments, please provide the information in the attached list **by November 14, 2022**. If the requested information has not yet been developed, please include the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the requested information, we will determine whether additional information is necessary to complete the review of the activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. Accordingly, until we complete our review, we request that the bank refrain from providing this service to its customers.

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 [REDACTED] at [REDACTED]. Written correspondence should be addressed to Kristie K. Elmquist, Regional Director, FDIC, Dallas 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: DALMailRoom@fdic.gov. Information about how to use secure email and FAQs about the service can be found at <https://www.fdic.gov/secureemail/>.

[REDACTED]

Page 2

Sincerely,

Kristie K. Elmquist
Regional Director

Attachment

cc: Federal Reserve Bank of Dallas

[REDACTED]

Crypto-Asset Activity Request List – [REDACTED]

Documentation:

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, [REDACTED], and any other related parties
6. The bank's permissibility analysis and determination with respect to the activity
7. Bank's analysis of SEC SAB 121 and its applicability
8. Cost-benefit analysis
9. Project plan
10. Vendor management due diligence documentation and analysis related to both [REDACTED] and [REDACTED], including audits, financials, insurance, complaints, etc.
11. Description of what happens to customers' accounts or holdings of Bitcoin, if the bank does not continue or cancels offering the services provided by [REDACTED]
12. Description of any fees that will be charged to consumers related to the activity, and how they will be calculated. Also, describe if and how fees are split amongst the bank and any third-parties involved in the activity.
13. Description of any transaction limitations imposed by [REDACTED] or the bank on the amount of Bitcoin a consumer may purchase or sell (e.g. daily, weekly, monthly)
14. Description of the methodology that determines the price consumer pays to [REDACTED] for bitcoin. This includes providing an explanation of how any market price is determined and how the spread, if any, is calculated.
15. Consumer 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)
16. 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 consumers by, or through, the bank in connection with activities.
17. Any other due diligence materials
18. Strategic plan that details how crypto-asset activity achieves objectives of the board and the contingency plan should the activity fail to achieve the objectives
19. 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.
20. Board and committee minutes reflecting discussion, analysis, approval, and any documentation provided on the activity
21. Risk assessment(s) related to the activity
22. Internal training materials related to the activity

23. Policies and procedures that will govern the crypto-related activity, including those related to consumer compliance and complaint resolution
24. 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).

DOCUMENT 22



Transmitted by Electronic Correspondence

October 17, 2022

President & COO

RE: Notification of Crypto-Related Activities

Dear [REDACTED]:

On July 8, 2022, we received your letter notifying the FDIC and [REDACTED] of your institution's involvement in crypto-related activities, in response 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.

We understand that in 2021, the Bank began exploring crypto-related activities and has decided to not offer crypto-asset products or services to Bank customers. The notification letter also stated that the Bank acquired three types of crypto-assets and subsequently exchanged less than \$25,000 in crypto-assets for Non-Fungible Tokens (NFT). Further, the notification letter says the Bank currently holds approximately \$1,300 worth of crypto-assets with a custodian. After a review of the Bank's notification letter, we have determined that additional information is needed to further clarify the crypto-related activities being conducted and crypto-related assets held by the Bank.

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 such activities. To assist in the review of the Bank's crypto-related activities, please provide the documentation listed below within 30 days of the date of this letter.

- Provide the Bank's most recent internal [REDACTED] Report reflecting crypto-assets and purchased NFTs, including volumes and values.

[REDACTED]

[REDACTED]

- [REDACTED]
- Explain the methods used to report and value (e.g., cost or fair value) the crypto-assets and NFTs on the Call Report. Provide supporting documentation and analysis. Include financial statement disclosures concerning these activities.
 - The Bank's 12/31/2021 [REDACTED] Report shows \$98,900 "[REDACTED]" held at [REDACTED] dollars. If U.S. Dollars, what is the purpose for holding this amount at [REDACTED] and for what purpose are the funds intended to be used? If [REDACTED] dollars, please clarify the discrepancy in the amount because the Bank reports \$1,300 in crypto-assets in the notification letter.
 - Please clarify whether the Bank owns any other crypto-assets or NFTs, other than what has already been disclosed.
 - Explain how the Bank uses the NFTs currently owned for promotional purposes and provide internal employee training material.
 - Please provide details about whether Directors and/or Officers of the Bank have a financial or other interest in the acquired NFTs.
 - Provide an independent legal analysis of the permissibility of the Bank acquiring and holding crypto-assets and NFTs under part 362 of the FDIC Regulations (12 CFR part 362) and other relevant state and federal laws.

Until we complete our review, we request the Bank refrain from purchasing additional crypto-assets and NFTs. When we have completed our review, we will provide the institution with relevant supervisory feedback, as appropriate.

Please notify us of any material changes in these activities or intent to engage in other crypto-related activities. 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). Questions should be directed to FDIC Case Manager [REDACTED] at [REDACTED] and [REDACTED] at [REDACTED].

Sincerely,

/s/ Kathy L. Moe

Kathy L. Moe
Regional Director
Federal Deposit Insurance Corporation

[REDACTED]
[REDACTED]
[REDACTED]

DOCUMENT 23


FDIC

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

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

Sent via secure email

October 21, 2022

Board of Directors

[REDACTED]
 [REDACTED]
 [REDACTED]

Subject: Notification of Engaging in Crypto-Related Activities

Dear Members of the Board:

During a virtual meeting held on May 6, 2021, President [REDACTED], Executive Vice President (EVP) and Chief Financial Officer [REDACTED], EVP and Chief Operating Officer [REDACTED], and other bank personnel presented and discussed the bank's then-newly announced partnership with [REDACTED] with staff of the FDIC and the [REDACTED]. During the meeting, bank management presented an overview of the relationship and planned activity to offer bank customers the ability to buy, hold, and sell Bitcoin through a mobile application. They also discussed management's risk assessment; the extent of contractual agreements; contemplated structure of the arrangements with [REDACTED] and the bank's core service provider [REDACTED]; planned timeframe for implementation; the extent of planned crypto asset offerings; and the holding company's investment in [REDACTED].

On April 4, 2022, during a virtual meeting, bank management provided an update to FDIC and [REDACTED] staff on the project and their ongoing due diligence. Bank management also provided additional documents and information on April 5, 2022, and June 8, 2022, in response to follow-up requests from the FDIC. On August 2, 2022, Chief Executive Officer [REDACTED] notified FDIC Field Supervisor [REDACTED] that the project had moved from a development phase to a testing phase as part of the bank's ongoing due diligence.

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 and outlined a supervisory feedback process concerning a bank's current or planned crypto-asset related activity. The FIL is available at <https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html>. 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 such activities. On October 6, 2022, the FDIC submitted a list of requested information to the bank,

Board of Directors
[REDACTED]

Page 2

which is currently under review as part of the examination that began on October 11, 2022. When we have completed our review, the FDIC will provide the bank with relevant supervisory feedback, as appropriate. Until we complete our review, we request that the bank refrain from providing this service to its customers.

Please notify us during our review period if there are any material changes in the planned service, the status of this project, or its planned implementation, to ensure that the bank is operating in a safe and sound manner and in compliance with consumer protection regulations.

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 related to Risk Management, please contact Assistant Regional Director Jaclyn Valderrama at [REDACTED] or Case Manager [REDACTED] at [REDACTED]. For questions related to Consumer Protection, please contact Assistant Regional Director Matthew Sheeren at [REDACTED] or 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 about 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

cc: [REDACTED]

Federal Reserve Bank of San Francisco

DOCUMENT 24



Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Division of Depositor and Consumer Protection
300 South Riverside Plaza, Suite 1700, Chicago, IL 60606

Chicago Regional Office
Phone (312) 382-7500
Fax (312) 382-6901

February 17, 2023

Board of Directors
[REDACTED]

Subject: Notification of Engagement in Blockchain Technology

Dear Members of the Board:

On September 28, 2022, the FDIC received notification of the bank's intent to partner with the [REDACTED] to offer [REDACTED]. The notification was provided pursuant to Financial Institution Letter (FIL)-16-2022, *Notification of Engaging in Crypto-Related Activities*. The FDIC requested additional information on December 13, 2022, to evaluate the safety and soundness, consumer protection, and financial stability considerations of the proposed activities.

The FDIC received the requested information from the bank on January 31, 2023. We will review the documents to determine whether subsequent information is necessary to evaluate the proposed activities. When we have completed our review, the FDIC will provide the bank with relevant supervisory feedback, as appropriate. Until we complete our review, we request that the bank refrain from providing the [REDACTED] and [REDACTED] to its customers.

Please notify us if there are any material changes in the planned service, the status of this project, or its planned implementation, to ensure that the bank is operating in a safe and sound manner and in compliance with consumer protection regulations.

This letter is confidential and may not be disclosed or made public in any manner under part 309 of the FDIC Rules and Regulations. If you have any questions, please contact Case Manager [REDACTED] at [REDACTED] or Senior Review Examiner [REDACTED] at [REDACTED].

Sincerely,
Gregory P. Bottone
Regional Director

cc: [REDACTED]
Federal Reserve Bank of Chicago

DOCUMENT 25



Federal Deposit Insurance Corporation
350 Fifth Avenue, Suite 1200
New York, New York 10118

New York Regional Office

May 5, 2023

Board of Directors

[REDACTED]

Subject: Information Request – Proposed Crypto-Asset Banking Activity

Dear Board Members:

On March 13, 2023, we received [REDACTED] (the Bank) notification of its intent to provide a bank account to [REDACTED] for the purpose of holding deposit reserves corresponding to [REDACTED] issuance of a stablecoin, [REDACTED] as requested in Financial Institution Letter (FIL), [FIL-16-2022, Notification of Engaging in Crypto-Related Activities](#).

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 such activities. In order to begin those assessments, please provide the information in the attached list by May 15, 2023. If the requested information has not yet been developed, please include the status and timeline for developing each item in the response, as applicable. Once the FDIC has completed its review of the requested information, we will determine whether additional information is necessary to complete the review of the proposed activity. When we have completed our review, the FDIC will provide the institution with relevant supervisory feedback, as appropriate. [REDACTED] should not proceed with any crypto-asset activity until such time that the FDIC has determined [REDACTED] ability to implement the activity in a safe and sound manner.

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 C.F.R. 309). If you have any questions, please contact Senior Case Manager [REDACTED] at [REDACTED] or Senior Review Examiner [REDACTED] at [REDACTED]. Written correspondence should be addressed to my attention at the New York Regional Office, and sent as a PDF document through the FDIC's Secure Email portal (securemail@fdic.gov) using the following e-mail address: NYMailroom@fdic.gov.

Sincerely,
Frank R. Hughes
Regional Director

Attachment: Crypto-Asset Activity Request List

cc: [REDACTED]

Crypto-Asset Activity Request List

1. Product and Key Initiative Risk Assessment, including considerations regarding applicable consumer compliance and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT)-related laws and regulations.
2. Due Diligence Memo and supporting documentation, including the [REDACTED] SOC1 report.
3. Board of Directors materials and minutes evidencing approval of the proposed activity.
4. Legal opinion on permissibility.
5. Brokered deposit applicability analysis.
6. Deposit volatility analysis.
7. Revisions to the contingency funding plan and other elements of liquidity risk management.
8. Liquidity stress testing analysis, both bank-wide and [REDACTED].
9. Wind down plan should [REDACTED] withdraw the [REDACTED] relationship from the Bank and a description of how a withdrawal has been incorporated into the contingency funding planning and liquidity stress testing.
10. Capital analysis, including a description of scenarios developed, assumptions, and methodology.
11. An updated description and information on the Bank's deployment of deposit funds received from [REDACTED] customers.
12. A description of any transactions between the proposed [REDACTED] reserve deposit account and the existing [REDACTED] payments account.
13. A description of procedures to monitor compliance with AML/CFT requirements, including customer identification and beneficial owner verification requirements at account opening.
14. Applicable client disclosures to end-users.
15. [REDACTED] marketing materials, including planned advertising, press releases, or other public statements, including any planned, drafted, or issued materials or media that contain the FDIC name or logo.
16. Describe any existing or expected statements or representations made regarding FDIC deposit insurance, including pass thru insurance, in association with any [REDACTED] deposits or any [REDACTED] customer deposits held at the Bank.
17. All (including drafts if not final) term sheets, binding commitments, and other agreements between the Bank and [REDACTED] including deposit account agreements (collectively, the Agreements).
18. If not addressed in the Agreements, describe any Bank responsibilities or obligations related to collateral requirements, balancing, verification, or attestation requirements (i.e. who is responsible for verifying the reserves are in place), and if [REDACTED] has any investment criteria.
19. A description of the timing of funds flowing from [REDACTED] to the Bank, and in reverse, the deposit and redemption of funds from purchases and redemptions of [REDACTED].
20. Describe whether or not the Bank has any explicit or implicit redemption obligations or there is a presumption that the Bank could be or is a redemption agent for [REDACTED] on either a wholesale or retail basis.
21. What percentage of [REDACTED] reserves could be held at the Bank? Is there a minimum or maximum?
22. Describe the Bank's expectations of future business relationship expansion with [REDACTED] given the partnership between [REDACTED] and [REDACTED].
23. Describe any expectations of [REDACTED] wallet integration/connection for the purpose of direct [REDACTED] redemptions by the Bank.

Chairman MEUSER. Thank you.
Mr. Thiel, you are now recognized for 5 minutes.

**STATEMENT OF FRED THIEL, CHAIRMAN OF THE BOARD OF
DIRECTORS AND CHIEF EXECUTIVE OFFICER, MARA**

Mr. THIEL. Chairman Meuser, Ranking Member Green, and distinguished members of the committee, thank you for the opportunity to testify on the critical issue of debanking of the digital asset ecosystem. I am honored today to be here to discuss the events that took place under Operation Choke Point 2.0 and the effects it had on the digital asset industry at large.

My name is Fred Thiel, and I serve as CEO of MARA, a leading company in the digital asset industry and the largest publicly traded Bitcoin miner. MARA is also the second largest corporate holder of Bitcoin. I am proud to say that MARA is dedicated to fostering U.S. economic growth, advancing domestic energy innovation, and bolstering U.S. national security through blockchain technology.

From revitalizing renewable energy assets and strengthening our power grids to mitigating methane emissions on oil fields and driving efficiency gains in high-performance computing applications like AI, MARA is fueling progress at the intersection of technology and industry. The employees that put on the MARA hat and go to work every day are a team comprised of veterans, blue-collar workers, technology and finance experts who contribute significantly to our local and national economies.

MARA invested nearly \$2 billion into the U.S. economy in 2024, including \$215 million investment in Nebraska, \$229 million investment in Ohio, and over \$1 billion investment in the State of Texas.

As CEO of MARA, I have had the privilege of being at the forefront of the digital asset industry's evolution over the last 5 years, witnessing firsthand its growth and impact on the future of finance.

The United States is not a stranger to the disruption and change that accompanies innovation. Our Nation has not only witnessed but led the development of transformative technologies like the internet, personal computers, and now artificial intelligence. Blockchain technology and digital assets represent yet another frontier of auspicious change that is already revolutionizing our daily lives.

Yet, despite the positive impact and promise of this technology, it is undeniable that the digital asset industry has been treated differently, singled out, and subjected to unprecedented actions that threaten to stifle America's leadership and innovation. Such discriminatory practices contradict our Nation's ethos of technological advancement and pose significant risks to our economic competitiveness and national security.

Today I am here to shed light on how these opaque, behind-the-scenes financial exclusion practices often occur without public scrutiny or legislative oversight, and if left unchecked, jeopardize the ability of legitimate businesses to operate within the United States, driving capital offshore. Clear, fair regulation must ensure that all companies that follow the law and play by the rules are treated fairly and have equal access to basic financial services. It is crucial

that we address these challenges to ensure America maintains its competitive edge in this rapidly evolving sector.

In 2023 and 2024, companies in the digital asset sector have experienced a disturbing pattern of financial exclusion by major banks, payment processors, and financial service providers. These actions taken without clear justification include the closure of commercial banking services, denial of lending and credit facilities, and exclusion from payment platforms. Discriminatory banking and financial policies harm the digital asset ecosystem and broader economic interests. By restricting access to essential services, banks and payment processors are determining which industries can thrive in the United States. These restrictions also undermine energy and national security goals as digital asset mining and blockchain technology are key to optimizing the energy grids and bolstering security.

Financial barriers slow investment in these critical solutions. Additionally, these practices violate free market principles allowing financial institutions to arbitrarily exclude legitimate industries, stifling competition, and setting a dangerous precedent for financial censorship.

To address these systematic abuses, I urge Congress to take several actions: First, ensure equal access to financial services by prohibiting blanket bans on digital asset companies, requiring individual risk assessments instead; second, increase regulatory transparency by mandating that financial institutions disclose reasons for account closures or denials, ensuring due process; third, promote a competitive financial ecosystem through clear regulations that allow digital asset businesses to operate without fear of arbitrary exclusion; finally, protect innovation by recognizing Blockchain's role in energy infrastructure and aligning financial policies with national security goals.

Some financial institutions have become increasingly welcome of cryptocurrencies and blockchain technology, recognizing the growing and strategic importance of digital assets. Some have established dedicated teams and divisions devoted to integrating this technology, expanding access to cryptocurrencies and investing in its future. I want to thank those who have partnered with our industry and have vocally advocated for clear frameworks that will provide necessary certainty to allow America to continue to innovate and lead the world on digital assets.

In conclusion, the financial debanking of digital asset ecosystems represents an existential threat to American leadership in technology, economic competitiveness, and national security. Without immediate action, legitimate businesses will continue to face discrimination, forcing innovation offshore, and reducing U.S. influence in a critical sector. I appreciate the committee's attention to this matter and look forward to answering any questions. Thank you.

[The prepared statement of Mr. Fred Thiel follows:]



Testimony of Frederick Thiel
CEO and Chairman of the Board

Before the Oversight and Investigations Subcommittee
United States House of Representatives

February 6, 2025

Chairman Meuser, Ranking Member Green, and distinguished Members of the Committee,

Thank you for the opportunity to testify on the critical issue of the debanking of the digital asset ecosystem. I am honored to be here today to discuss the events that took place under Operation Choke Point 2.0 and the effects it had on the digital asset industry at large.

Introduction

My name is Fred Thiel, and I serve as CEO of MARA, a leading company in the digital asset industry and the largest publicly traded Bitcoin miner. MARA is also the second largest corporate holder of bitcoin. I am proud to say that MARA is dedicated to fostering U.S. economic growth, advancing domestic energy innovation, and bolstering U.S. national security through blockchain technology. From revitalizing renewable energy assets and strengthening our power grids to mitigating methane emissions on oil fields and driving efficiency gains in high-performance computing applications, like AI, MARA is fueling progress at the intersection of technology and energy.

The employees that put on the MARA hat and go to work every day are a team comprised of veterans, blue-collar workers, and technology and finance experts who contribute significantly to our local and national economies. We invested nearly \$2 billion into the U.S. economy in 2024, including a \$215 million investment in Nebraska, a \$229 million investment in Ohio, and a \$1 billion investment in Texas.

As CEO of MARA, I have had the privilege of being at the forefront of the digital asset industry's evolution over the last five years, witnessing firsthand its growth and impact on the future of finance. The United States is no stranger to the disruption and change that accompanies innovation. Our nation has not only witnessed but led the development of transformative technologies like the internet, personal computers, and now artificial intelligence. Blockchain technology and digital assets represent yet another frontier of auspicious change that is already revolutionizing our daily lives.

Yet, despite the positive impact and promise of this technology, it is undeniable that the digital asset industry has been treated differently – singled out and subjected to unprecedented actions that threaten to stifle America's leadership in innovation. Such discriminatory practices contradict our nation's ethos of technological advancement and pose significant risks to our economic competitiveness and national security.

Today, I'm here to shed light on how these opaque, behind-the-scenes financial exclusion practices often occur without public scrutiny or legislative oversight, and if left unchecked, jeopardize the ability of legitimate businesses to operate within the United States, driving economic opportunities offshore. Clear, fair regulation must ensure that all companies that follow the law and play by the rules are treated fairly and have equal access to basic financial services. It is crucial that we address these challenges to ensure America maintains its competitive edge in this rapidly evolving sector.

The Systematic Financial Exclusion of the Digital Asset Industry

In 2023 and 2024, companies in the digital asset sector have experienced a disturbing pattern of financial exclusion by major banks, payment processors, and financial services providers. These actions, taken without clear justification, include the closure of commercial banking services, denial of lending and credit facilities, and exclusion from payment platforms.

MARA specifically has faced a pattern of financial exclusion resulting from discriminatory banking and financial practices targeting crypto-related companies. These actions have disrupted operations and required burdensome workarounds in order for MARA to compete on a global stage – despite our full compliance with local, state and federal laws and regulations.

For instance, MARA has been recognized as a company in good standing by the state of Nevada since 2010. We are an SEC registrant and therefore subject to significant regulation by the SEC. We are audited rigorously by a national independent CPA firm and frequently engage in transactions that require robust due diligence of our company. Auditors, regulators, and transactional counterparties are continually vetting MARA. At every level, MARA is held to the highest legal, regulatory and industry standards – and we meet them without exception.

Forced Bank Account Closures

Forced bank account closures have been a significant issue in the digital asset industry since 2023. Multiple financial institutions have abruptly closed accounts of digital asset firms, citing unclear risk concerns rather than any compliance deficiencies. In some cases, companies were given extremely short windows to relocate funds, disrupting normal business operations. Additionally, companies attempting to open new commercial banking accounts have faced rejections despite meeting all regulatory and compliance requirements. Some institutions have explicitly stated that they have policies against servicing digital asset-related businesses, regardless of financial health or compliance standing.

Denial of Credit and Lending Services

The denial of traditional credit and lending services has also been a major challenge for the industry historically. Digital asset companies have been denied access to traditional credit, even in cases where they have offered fully collateralized guarantees. Financial institutions have cited internal policies prohibiting lending to companies in the sector, effectively cutting off capital needed for business expansion and innovation. Furthermore, companies seeking traditional lines of credit for operational expenses, travel, and business development have been denied services solely due to their industry affiliation, forcing them to find less efficient alternatives.

Payment Services Restrictions

Payment services restrictions have further compounded these difficulties. Certain payment platforms and fintech services have explicitly restricted access for digital asset companies, making it more difficult to conduct routine business transactions. Moreover, some firms in the sector have been unable to obtain corporate credit card accounts due to blanket risk policies that exclude digital asset businesses without consideration of individual companies' financial profiles.

Impact on Innovation, Economic Growth, and National Security

These discriminatory banking and financial policies threaten the digital asset ecosystem and broader economic interests. By restricting access to essential financial services, banks and payment processors are effectively deciding which industries can exist and grow within the U.S. economy. This situation is driving U.S. innovation offshore, as companies in the digital asset industry that contribute to

technological advancements, job creation, and economic growth are forced to consider offshore banking options, pushing innovation and capital outside the United States.

Furthermore, these restrictions are undermining U.S. energy and national security goals. Digital asset mining and blockchain technology are critical tools for optimizing energy grids and supporting national security. Financial restrictions on the industry slow down investments in these innovative energy solutions. Additionally, these practices violate free market principles, as financial institutions should not be in the business of arbitrarily deciding which legitimate industries can operate. The systematic exclusion of digital asset companies undermines market competition, disrupts businesses, and sets a dangerous precedent for financial censorship.

Policy Recommendations

To address these systemic abuses, I urge Congress to consider several actions. These include ensuring equal access to financial services by prohibiting banks from implementing industry-wide bans on providing banking and lending services to digital asset companies without individual risk assessments. Increasing regulatory transparency by requiring financial institutions to disclose reasons for account closures or denials, ensuring due process for affected businesses, is also recommended. Fostering a competitive financial ecosystem by encouraging regulatory clarity that allows digital asset businesses to operate within the U.S. without fear of arbitrary exclusion is crucial. Lastly, protecting innovation and energy optimization by recognizing the role of blockchain and digital asset technology in supporting energy infrastructure and ensuring financial policies align with national security goals is essential for the industry's growth and contribution to the broader economy.

Partnering with Financial Institutions

Some financial institutions have become increasingly welcoming of cryptocurrencies and blockchain technology in recent months, recognizing the growing and strategic importance of digital assets. Many have even established dedicated teams and divisions devoted to integrating this technology, expanding access to cryptocurrencies and investing in its future. I want to thank those who have partnered with our industry and have vocally advocated for clear regulatory frameworks that will provide the necessary certainty to allow America to continue to innovate and lead the world on digital assets.

Conclusion

The financial debanking of the digital asset ecosystem represents an existential threat to American leadership in technology, economic competitiveness, and national security. Without immediate action, legitimate businesses will continue to face discrimination, forcing innovation offshore and reducing U.S. influence in a critical sector.

I appreciate the Committee's attention to this matter and look forward to answering any questions. Thank you.

Chairman MEUSER. Thank you, Mr. Thiel.
 Ms. Olesiuk, you are now recognized for 5 minutes.

**STATEMENT OF SHAYNA OLESIUK, DIRECTOR OF BANKING
 POLICY, BETTER MARKETS**

Ms. OLESIUK. Good afternoon, Chairman Hill, Chairman Meuser, Ranking Member Waters, and Ranking Member Green, and members of the subcommittee. Thank you for the invitation to testify today. My name is Shayna Olesiuk, and I am the Director of Banking Policy at Better Markets. Better Markets is a nonprofit, non-partisan, independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support financial reforms of Wall Street, and make the financial system work for all Americans again.

I have more than 25 years of experience in the financial services and banking regulatory area. I have led and participated in projects related to banking regulatory policy, systemic risk, the provision of banking services and products to all Americans, including underserved consumers and communities.

The topic of today's hearing is of vital importance, whether or not regulators will conduct unbiased, risk-based analysis regardless of the source of risk to the banking system. What is really at stake is protecting our financial system and main street Americans from the risks, costs, and consequences of incredibly volatile and often flagrantly illegal conduct and criminal activity. Many crypto companies have put themselves in the crosshairs by choosing to engage in or enable these activities.

If the crypto industry had followed the law, like almost every other financial firm in the United States, then it would not be crosswise with the regulators who are mandated to enforce the law and protect consumers, investors, and financial stability. This is also an issue of fairness to the other financial firms in the United States who are following the law. Crypto should not be given an unfair advantage over its competitors with a different set of rules.

The explosive growth of crypto in recent years has massively endangered the financial system in ways we have never seen. Banks and other financial firms have become involved with crypto firms, and several have experienced devastating failures. These failures harmed the banking system and bank customers and came with an enormous price tag of \$40 billion in direct costs—that is billion with a “B”—and threatened financial stability. Furthermore, main street Americans are being misled and defrauded into believing that crypto is ensured by the FDIC, which is a completely false claim.

Financial experts, regulators, and law enforcement all recognize the very real risk that crypto presents to the banking industry and financial stability. For instance, the Federal Bureau of Investigations (FBI) received more than 69,000 reports of financial fraud involving crypto in the year 2023 alone, with estimated losses to real people of \$5.6 billion. Even hedge fund titan Elliott Management has sounded an unprecedented alarm about the speculative frenzy in the crypto markets.

None of this is to dispute that access to the banking services is an important goal to support the functioning of our economy and

benefit all Americans. Regulators have two fundamental duties in this area: First, regulators have a duty to ensure that banks comply with applicable laws; second, regulators must promote safe and sound banking practices and must take corrective action when banks engage in unsafe and unsound practices.

The bottom line here is that regulators and banks must act in the best interest of the public and main street Americans. The facts and evidence show that standing with crypto often means standing with those who engage in high-risk, if not illegal and criminal activities, with a highly volatile product that has no legitimate social use and could endanger the entire financial system and ultimately the economy. These are very real risks.

Having so recently suffered from the catastrophic 2008 financial crash, enabled and fueled by unregulated novel and innovative financial products, the American people deserve that protection. Thank you, and I look forward to your questions.

[The prepared statement of Ms. Olesiuk follows:]



Testimony of Shayna Olesiuk
Director of Banking Policy, Better Markets, Inc.
Before
The U.S. House Committee on Financial Services
Oversight and Investigations Subcommittee

“Operation Choke Point 2.0:
The Biden Administration's Efforts to Put Crypto in the Crosshairs”

February 6, 2025

Good afternoon, Chairman Meuser, Ranking Member Green, and Members of the Subcommittee. Thank you for the invitation to testify today.

My name is Shayna Olesiuk, and I am the Director of Banking Policy at Better Markets, Inc. (“Better Markets”), a non-profit, non-partisan, and independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support financial reforms of Wall Street, and make the financial system work for all Americans again.

Better Markets works with allies to promote pro-market, pro-business, and pro-growth policies that help build a stronger, safer financial system, one that protects and promotes Americans’ jobs, savings, retirements, and more. Better Markets has filed more than 500 comment letters with U.S. banking, securities, and derivatives regulators, many addressing the implementation of the Dodd-Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank Act”).¹ We have also published numerous letters, reports, fact sheets, and white papers on public policy issues pertinent to the U.S. banking sector and had hundreds of meetings with U.S. regulators and others. Much of our attention has focused on critical issues before this Committee, including ensuring that the financial system (1) supports the real economy, jobs, economic growth, small businesses, and community banks (2) is resilient, not prone to crashes, and strong enough never to need bailouts; (3) protects workers, consumers, investors, and markets; (4) reduces wealth and income inequality; and (5) is designed withstand the consequences of any material financial risk including those caused by the climate crisis. Our website, www.bettermarkets.org, includes information on these and our other public interest activities.

I have more than 25 years of experience in financial services and banking regulatory work. In my current role, I lead and participate in advocacy projects related to banking regulatory policy, systemic risk, racial justice, and the interests of low-and moderate-income consumers and communities. Previously, I worked at the Federal Deposit Insurance Corporation where most recently I was a Deputy Director in the Division of Insurance and

¹ Public Law 111-203, 124 Stat. 1376 (2010).

Research. Earlier in my career, I worked at the Federal Reserve Bank of San Francisco. In each of these roles, I have focused on ensuring that the banking industry and financial system work for Main Street Americans. I hold degrees in Economics and Business Administration: Financial Services from Saint Mary's College of California and am a CFA® charterholder. I grew up in a small town in Northern California. Further information on my background and work can be found [here](#).

Table of Contents

Introduction.....	3
Background	6
Definition and History.....	6
Irrelevance and Distrust.....	7
Valuation and Volatility.....	8
2024 Election Influence	9
Key Dangers of Crypto	10
Crypto Valuations are Volatile.....	10
Crypto Causes Bank Runs	12
Crypto Enables Fraud	13
Crypto Harms Minorities and Underserved Communities.....	14
Crypto Is Not Protected by FDIC Deposit Insurance	16
Regulatory Responsibilities	17
Existing Risk Management Principles.....	17
Bank Secrecy Act.....	18
Bank-Fintech Partnerships with Crypto Firms & Related Deposit Insurance Concerns	19
Recommendations.....	20
More Clarity on the Rules and Expectations of Banks	20
Greater Disclosure Requirements for Banks	20

Introduction

Like all lawbreakers, the crypto industry put itself in the “crosshairs” of regulators and prosecutors when it chose to engage in widespread, flagrant illegal conduct, enable and facilitate criminal activity, and refuse to adhere to the most basic, fundamental customer, investor and financial stability protections. As discussed below, if the crypto industry had followed the law like almost every other financial firm in the U.S., then it would not have been crosswise with regulators and prosecutors who are mandated to enforce the law and protect customer, investor and financial stability. This is also an issue of fairness to the other financial firms in the U.S. who are following the law. Crypto should not be given an unfair advantage over their competitors.

These rules and laws are fundamental protections not just for financial customers, investors, and markets, but for all hardworking Americans whose economic security, opportunity, and prosperity are endangered by financial instability. The leading recent example of this are the jobs, homes, savings, retirements, and dreams of tens of millions of Americans that were lost due to the financial crisis of 2007-2009 (“2008 Crash”).² These innocent victims of an unregulated financial system highlight the critical importance of having strong regulations combined with effective and assertive supervisory oversight to ensure the largest financial firms are both resilient and safely run. Pre-crisis banking rules for the largest banks were woefully deficient and ineffective. Weak standards allowed large banks to take too much risk, contributing to a crisis that had devastating effects on Main Street families and businesses. At the same time, banking supervision—the day-to-day oversight of these firms that should complement and fill in potential gaps in rules to ensure banks are not dangerously run—failed dramatically, and combined with the weak rules, created a particularly fragile banking system with disastrous consequences.

The explosive growth of digital assets and cryptocurrency in recent years³ has massively endangered the banking system in ways we have never seen, or even conceived. Banks have become involved with crypto firms, and several—namely Signature Bank (“Signature” or “SBNY”), Silicon Valley Bank (“SVB”) and Silvergate Bank (“Silvergate”)—have experienced devastating failures⁴ that harmed the banking industry and bank customers, imposed significant costs on taxpayers and the public, and threatened financial stability. Clearly, crypto and the risks it brings have the potential to spark a full-scale banking

² BETTER MARKETS, THE COST OF THE CRISIS (July 2015), <https://bettermarkets.org/newsroom/20-trillion-cost-financial-crisis-3>.

³ See, e.g., FINANCIAL STABILITY OVERSIGHT COUNCIL, REPORT ON DIGITAL ASSET FINANCIAL STABILITY RISKS AND REGULATION 9 (2022), <https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf>; Arthur E. Wilmarth, *We Must Protect Investors and Our Banking System from the Crypto Industry*, 101 WASH. U. L. REV. 235 (May 31, 2023), <http://dx.doi.org/10.2139/ssrn.4360175>.

⁴ CONGRESSIONAL RESEARCH SERVICE, THE ROLE OF CRYPTOCURRENCY IN THE FAILURES OF SILVERGATE, SILICON VALLEY, AND SIGNATURE BANKS (Apr. 25, 2023), <https://crsreports.congress.gov/product/pdf/IN/IN12148>.

crisis which could, in fact, be much faster moving and more devastating than the 2008 Crash.

Main Street Americans who were misled or defrauded into believing that cryptocurrency is insured by the Federal Deposit Insurance Corporation (“FDIC”) have also been seriously harmed. False statements suggesting that crypto is insured by the FDIC are blatantly illegal, but often the harm done by these statements to everyday Americans cannot be undone.⁵ The safety and soundness of the financial system is also put at risk because if people question the applicability of FDIC insurance then they will precipitously withdraw their deposits and cause a run on the banking system.

Financial experts and regulators have recognized the risk that cryptocurrencies present to the banking industry and financial stability. For example, the Financial Stability Oversight Council (“FSOC”) named digital assets and crypto as a key vulnerability in its 2024 Annual Report because of the threats it presents to the financial system.⁶ The Congressional Research Service (“CRS”), Office of the Inspector General (“OIG”) of the Federal Reserve Board (“Fed”), and FDIC have studied the role of crypto in the 2023 bank failures and raised questions about the ability of banks to manage the immense risk of crypto.⁷ Economists at the Federal Reserve Bank of New York (“New York Fed”) detailed the financial stability risks stemming from crypto—specifically its inherent volatility and susceptibility to bank runs.⁸ The Federal Bureau of Investigation (“FBI”) recently reported that more than 69,000 complaints related to financial frauds involving crypto were received in 2023, with estimated losses totaling \$5.6 billion.⁹ Even hedge funds, operating outside of the government and

⁵ See, e.g., Shayna Olesiuk, *Bank-Fintech Partnerships Hold Promise but Banking Agencies Must Do More to Protect the Public*, Better Markets (Oct. 30, 2024), https://bettermarkets.org/wp-content/uploads/2024/10/Better_Markets_Fact_Sheet_Fintech_Bank_Partnerships-10.30.24.pdf; Better Markets Comment Letter, *Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses* (Oct. 30, 2024), <https://bettermarkets.org/wp-content/uploads/2024/10/Better-Markets-Comment-Letter-RFI-Bank-Fintech-Arrangements.pdf>.

⁶ FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT at 8-9 and 45-46 (2024), <https://home.treasury.gov/system/files/261/FSOC2024AnnualReport.pdf>.

⁷ See, e.g., CONGRESSIONAL RESEARCH SERVICE, *supra* note 4; BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REVIEW OF THE FEDERAL RESERVE’S SUPERVISION AND REGULATION OF SILICON VALLEY BANK (Apr. 2023), <https://www.federalreserve.gov/publications/files/syb-review-20230428.pdf>; OFFICE OF THE INSPECTOR GENERAL, REVIEW OF THE SUPERVISION OF SILVERGATE BANK (Sept. 27, 2023), <https://oig.federalreserve.gov/reports/board-review-silvergate-summary-sep2023.pdf>; FEDERAL DEPOSIT INSURANCE CORPORATION, FDIC’S SUPERVISION OF SIGNATURE BANK (Apr. 28, 2023), <https://www.fdic.gov/sites/default/files/2024-03/pr23033a.pdf>.

⁸ Pablo D. Azar, et al., *The Financial Stability Implications of Digital Assets*, 30 ECONOMIC POLICY REVIEW (Nov. 2024), https://www.newyorkfed.org/medialibrary/media/research/epr/2024/EPR_2024_digital-assets_azar.pdf.

⁹ FEDERAL BUREAU OF INVESTIGATION, CRYPTOCURRENCY FRAUD REPORT 5 (Sept. 9, 2024), https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf.

regulatory agencies, have recognized and warned of the dangers of speculative investor frenzy in crypto markets.¹⁰

Access to banking services is an important policy goal that supports the functioning of our economy and benefits all Americans. Access to banking services should be available in all local communities, including rural and underserved communities, and to law-abiding businesses.

The terms “debanking” or “derisking” are sometimes used in a factual sense to refer to banks closing accounts based on the risk profile of a customer. For example, a bank may determine an account appears to be being used for illegal purposes and may then decide to close the account. “Debanking” is sometimes used in a different sense to describe the alleged exercise of regulatory authority to discourage banks from providing services to certain classes of customers, based on ideological or policy goals, separate from a risk-based analysis and determination.

Regulators have two fundamental duties in this area:

- First, regulators have a duty to ensure that banks comply with applicable laws, and;
- Second, regulators must promote safe and sound banking practices, and take corrective action when banks engage in unsafe and unsound practices.

In other words, banks must always understand and manage **any risk** that they are accepting in their business decisions. Banks cannot evade this responsibility by entering into business partnerships with third parties.¹¹ Banks can be, and frequently have been, subject to formal regulatory consent orders because of third-party partners’ violations of law in connection with activities performed on the bank’s behalf.¹² These have included violations of laws intended to protect consumers and, most frequently, violations of the Bank Secrecy Act, which is intended to safeguard the financial system against being used

¹⁰ Costas Mourselas, *Hedge fund Elliott warns White House is inflating crypto bubble that ‘could wreak havoc’*, FINANCIAL TIMES (Jan. 30, 2025), <https://www.ft.com/content/5fe69580-7f01-4215-98bb-b6ec5f7cd833>.

¹¹ See 12 U.S.C. § 1867(c)(1) which states, “[W]hen a depository institution that is regularly examined by an appropriate Federal banking agency . . . causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises . . . such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises”

¹² Better Markets Comment Letter, *supra* note 5. Better Markets conducted a best-efforts review of formal agency enforcement actions that were issued between January 1, 2023, and August 31, 2024, and identified 29 actions that included language directing the recipient to take some action related to third-party risk.

for illicit activity. These enforcement actions are published on agency websites for all to see. Regulators taking these actions are doing the job Congress mandated to protect the public.

Furthermore, regulators must apply corrective actions when banks take on unacceptable levels of risk or engage in activities that endanger the public interest. In some cases, regulators have taken enforcement actions for risks arising from a bank's failure to adequately manage risks arising from its third-party relationships. These actions are consistent with regulators' statutory mandate to ensure a safe and sound banking system.

In short, what's really at stake here is the responsibility of regulators and banks to act in the best interest of the public and Main Street Americans. The facts and evidence show that standing with crypto means standing with those who engage in very high risk if not illegal and criminal activities with a highly volatile product that has no legitimate social use and that could endanger the entire financial system and, ultimately, the economy. These are very real risks that the law mandates regulators require banks to eliminate or mitigate to the greatest extent. Having so recently suffered from the 2008 catastrophic financial crash enabled and fueled by unregulated, novel, and innovative financial products, the American people deserve that protection.

Background

Definition and History

By definition, crypto is a specific type of digital asset that depends on technology to support the security of a financial transaction.¹³ While crypto has existed for nearly two decades and offered numerous promises of innovation and other benefits that will improve the financial system, the promises have not materialized.

Since the publication of the Bitcoin whitepaper in 2008,¹⁴ crypto developers have created thousands of cryptocurrencies. Together, these developers and their venture capital backers have spun a narrative that these projects would revolutionize everything in modern life from finance to the internet. Yet, after nearly two decades since the creation of Bitcoin, and billions of dollars in venture capital investment, the promised golden goose has yet to yield any golden eggs.¹⁵ In fact, not only has cryptocurrency come up empty on its promises, but it also is yet to be determined if any cryptocurrency will ever yield any

¹³ FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT 98 (2022), <https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf>.

¹⁴ Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 31, 2008), <https://bitcoin.org/bitcoin.pdf>.

¹⁵ Better Markets, *The Golden Goose That Never Laid Golden Eggs: Unfulfilled Promises of Cryptocurrencies* (July 2023), https://bettermarkets.org/wp-content/uploads/2023/07/Better_Markets_Unfulfilled_Promises_Crypto_July2023.pdf.

substantive use case in the future. So far, its primary accomplishment has been to inflict excruciating losses on millions of investors who have seen billions of dollars disappear in fraudulent crypto schemes and ensuing bankruptcies.

Crypto proponents argue for the uniqueness of their products, asserting that existing financial regulations do not apply to them. However, this claim is fundamentally flawed. The reality is that many crypto tokens fall squarely within the definitions of securities as established by law. Historical precedents show that industries attempting to sidestep regulation, whether through innovative financial products or technological advancements, have consistently failed to secure exemptions from the very laws designed to protect investors.

The argument against regulatory compliance is often couched in terms of innovation and progress. Yet, this narrative conveniently ignores the implications of a lawless financial landscape. Crypto exchanges find themselves embroiled in legal battles for operating as unregistered broker-dealers, custodians, and exchanges. They do not adhere to the decades-old compliance standards required of traditional financial institutions, undermining the trust that underpins our capital markets and putting investors at risk.

Irrelevance and Distrust

A CNBC poll¹⁶ from late 2022 found that just 8% of Americans had a positive view of cryptocurrencies while a 2024 Harris poll¹⁷ found that 69% of likely voters in swing states held negative views of crypto. The industry likes to claim that 52 million Americans own crypto, but that figure comes from a deceptive poll paid for by the industry.¹⁸ The actual figure, according to data from the Fed, is closer to 18 million Americans¹⁹—and that number

¹⁶ Steve Liesman, *Just 8% of Americans have a positive view of cryptocurrencies now, CNBC survey finds*, CNBC (Dec. 7, 2023), <https://www.cnbc.com/2022/12/07/just-8percent-of-americans-have-a-positive-view-of-cryptocurrencies-now-cnbc-survey-finds.html>.

¹⁷ HARRIS POLL INSIGHTS, *CRYPTO ATTITUDES IN SWING STATES* 11 (May 7, 2024), https://theblockchainassociation.org/wp-content/uploads/2024/05/DCG_HarrisPoll-Research-Report.pdf.

¹⁸ Better Markets, *Proceed with Caution: Deceptive Polling Paid-for by the Cryptocurrency Industry* (July 2023), https://bettermarkets.org/wp-content/uploads/2023/07/BetterMarkets_Deceptive_Polling_Paid-For_ByCrypto_July2023-1.pdf.

¹⁹ See BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2023*, at 37 (May 2024), <https://www.federalreserve.gov/publications/files/2023-report-economic-well-being-us-households-202405.pdf>; Eddie Mitchell, *7% of Americans Hold Cryptocurrencies, Says Fed— Is 40% Claim Just Crypto Industry Wishful Thinking?*, CCN (Aug. 6, 2024), <https://www.ccn.com/news/crypto/americans-cryptocurrencies-fed-40-crypto-industry-wishful/>.

is declining. Moreover, of the Americans who own crypto, a mere 1% used it in 2023 to buy something, down from 2% in 2022.²⁰

So, nearly two decades after the creation of Bitcoin and billions of dollars in venture capital investment, the crypto industry still has no socially acceptable use. The industry has made claims that it would make our financial system more inclusive, serve as a payment mechanism and/or serve as a hedge against inflation. These claims, and many more, have proven to be baseless.²¹

The least disreputable use for crypto continues to be gambling and wild speculation. It remains a key tool for tax evaders, money launderers, ransomware, organized crime syndicates, foreign terrorist organizations, and state-sponsored actors on behalf of rogue states like North Korea and Iran. It also enables fraud and scams that have stolen hundreds of millions of dollars from the American people.²²

Valuation and Volatility

The extreme rise and fall in the value of crypto shows its volatility. After modest beginnings, the market capitalization, or total supply of crypto based on the current market price, reached a peak near \$3 trillion in 2021 but then quickly lost nearly two-thirds of its value with a fall back to about \$1 trillion in 2022 (see Chart 1).²³ Following the 2024 presidential election, the crypto market again soared above \$3 trillion.²⁴

²⁰ BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 19.

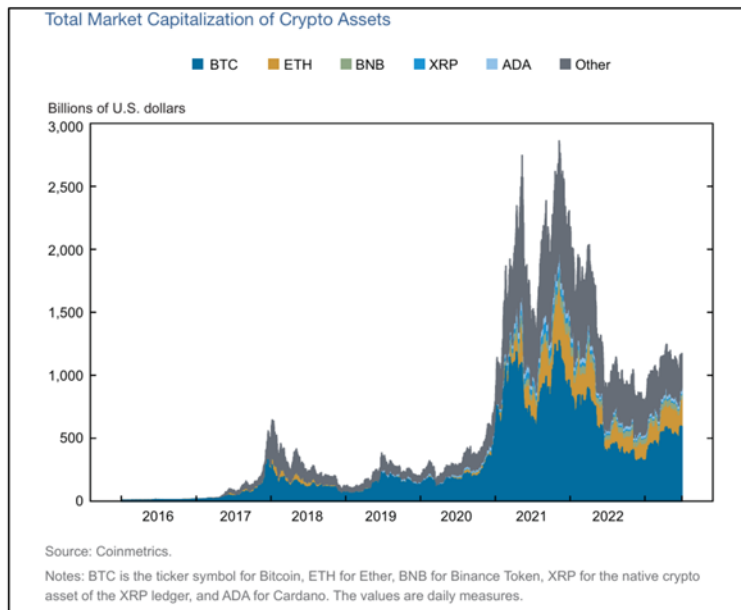
²¹ Better Markets, *Crypto 101: Bait-and-Switch, False Promises, Influence Peddling and a Growing Threat to our Financial System and Main Street* (Nov. 14, 2024), https://bettermarkets.org/wp-content/uploads/2024/11/Better_Markets_Crypto_Lame_Duck_Fact_Sheet-11.14.24.pdf.

²² *Id.*

²³ Azar et al., *supra* note 8, at 11.

²⁴ Will Schmitt, *Value of global crypto market tops \$3tn for first time in three years*, FINANCIAL TIMES (Nov. 11, 2024), <https://www.ft.com/content/4e304f28-4caf-4fbf-987c-17fc6de4fc4a>.

Chart 1



2024 Election Influence

The crypto industry spent almost \$200 million on campaign ads during the 2024 election.²⁵ While crypto spent big on ads attacking skeptical lawmakers, they never actually mentioned crypto.²⁶ This is the equivalent of Ford or Chevrolet running an ad campaign that never mentions cars or trucks!

This is because the crypto industry has a long record of lawbreaking and enabling outrageous crimes like ransomware and money laundering, which is why American voters are rightfully distrustful of crypto. The industry spent hundreds of millions of dollars to eliminate lawmakers who stand up for consumers and the public interest but never mentioned the real reason they are trying to defeat these candidates. What are they trying

²⁵ Brady Dale, *No crypto talk in the election ads crypto paid for*, AXIOS (Oct. 29, 2024), <https://www.axios.com/2024/10/29/crypto-election-ad-spend-fairshake-pac>.

²⁶ Better Markets, *supra* note 21.

to buy with that money? Crypto's top goal is to get its special interest legislation passed to give the industry an aura of legitimacy, despite its long history of deceit and lies.

Key Dangers of Crypto

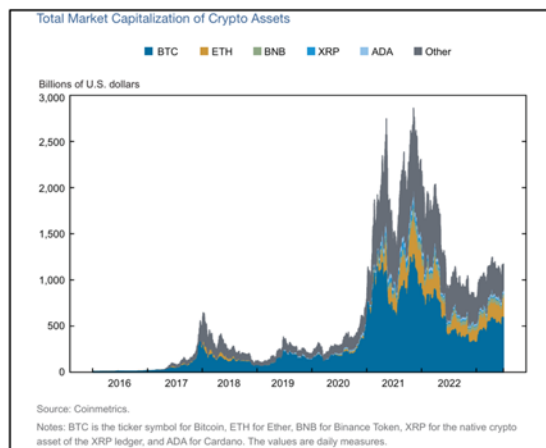
Unlike the benefits of convenience, cost savings, and security that the crypto industry would like the public to see, the truth is that crypto presents a long list of risks that endanger American families, banks, the financial system, the economy, and financial stability, including:

- Valuation volatility,
- Vulnerability to runs,
- Fraud,
- Harm to minorities and underserved communities, and
- False claims of FDIC deposit insurance protection.

Crypto Valuations are Volatile

The total value of crypto in circulation skyrocketed from around \$250 billion in 2000 to \$3 trillion in 2021 and then subsequently fell back to around \$1 trillion in 2022 (see Chart 1).²⁷

Chart 1



²⁷ Azar et al., *supra* note 8, at 11.

In late 2024, following the presidential election, the crypto market cap again reached \$3 trillion driven in part by the perceived support that crypto has in the Trump administration.²⁸ Not only is crypto incredibly volatile over the course of several years, but it has also been volatile from day to day. For example, Bitcoin's value has dropped 30% in a single day.²⁹ Industry observers offer many explanations for crypto's volatility:

[Crypto] isn't intrinsically valuable. There isn't gold or diamonds or anything backing up crypto's value. At no point did the U.S. Treasury say, 'Yes, any time someone wants to bring us Bitcoin, we will give them X number of dollar bills from our reserves.' Not all die-hard crypto fans would agree, but there is an argument that crypto's value really only comes from how much people are willing to trade for it—in goods, other cryptocurrencies, or in dollars.

Let's unpack this.

There are investors who are interested in crypto not to use it as a currency, but to use it as a hedge against inflation, or as an investment vehicle. ***But without anything intrinsically valuable backing up the currency, crypto's market value is based entirely on speculation, which is essentially educated guesswork.***³⁰

While some investors undoubtedly have benefited from gains during crypto booms, the frequent and significant crashes that follow leave many if not most investors vulnerable to heavy losses. Crypto's volatility creates opportunities for some traders to gain, but just as many, if not more, traders face significant losses, especially those who borrow money (leveraged trading) to trade.

One might look at the price increases and decreases in crypto over the long term and conclude that they balance each other out. Unfortunately, that is only true for a steadfast buy-and-hold purchaser, not for those who trade in and out of the crypto market at different times (sometimes being forced to do so during price movements that require a leverage crypto owner to add more funds to cover their positions). ***That volatility can and often does lead to significant losses.***

²⁸ Schmitt, *supra* note 24.

²⁹ Ryan Browne & Arjun Kharpal, *Bitcoin plunges 30% to \$30,000 at one point in wild session, recovers somewhat to \$38,000*, CNBC (May 18, 2021), <https://www.cnbc.com/2021/05/19/bitcoin-btc-price-plunges-but-bottom-could-be-near.html>.

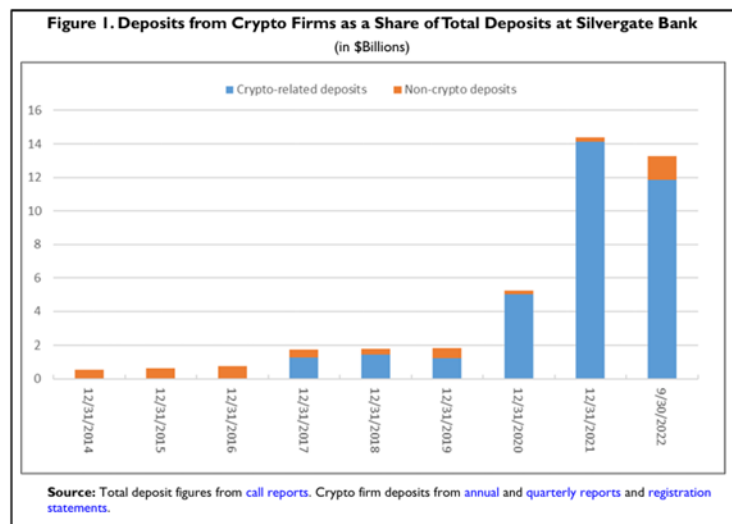
³⁰ Nicole Lapin, *Explaining Crypto's Volatility*, FORBES (Apr. 21, 2022), <https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility/>.

Crypto Causes Bank Runs

It is well-known and has been well-documented that exposure to crypto was a common cause of the failures of Signature, SVB, and Silvergate.³¹ For example, a CRS report called the phenomena “*the manifestation of crypto market volatility affecting traditional finance.*”³²

The CRS detailed how all three banks held deposits or made loans to the crypto industry. For example, at one point before its liquidation, 98% of Silvergate’s deposits were crypto-related (see Chart 2).³³

Chart 2



Not only was the failed banks’ direct exposure to crypto a catalyst for their failure, but the exposure caused second-order panic among non-crypto customers who recognized the risk and pulled their deposits from the failing banks, only accelerating their demise. For example, the FDIC’s post-mortem report of Signature’s failure details the toxic combination

³¹ See, e.g., CONGRESSIONAL RESEARCH SERVICE, *supra* note 4.

³² *Id.*

³³ *Id.* at 2.

of reputation risk related to the inherent volatility of crypto, inadequate management, and crypto exposure:

SBNY's significant client concentration of digital asset companies put it in a precarious position when the "crypto winter" hit in 2022. News articles scrutinized SBNY's involvement in the industry. SBNY experienced depositor run-off from both crypto customers as well as traditional depositors. However, management did not acknowledge that its exposure to the crypto industry might entice other customers to pull or reduce their own deposits. . . .

SBNY management countered a Wall Street Journal article in a January 23, 2023, press release, trying to correct the perception that SBNY was a "crypto lender" or that it invested in, held, or was a custodian of crypto assets. . . .

On March 10, 2023, SBNY began to experience deposit withdrawals, with deposit outflows accelerating significantly after the announced closure of SVB. SBNY did not have sufficient cash to fulfill its large volume of deposit withdrawal requests, which equaled 20 percent of total deposits. SBNY was unprepared for and unable to enact contingency plans against the large deposit withdrawal requests.³⁴

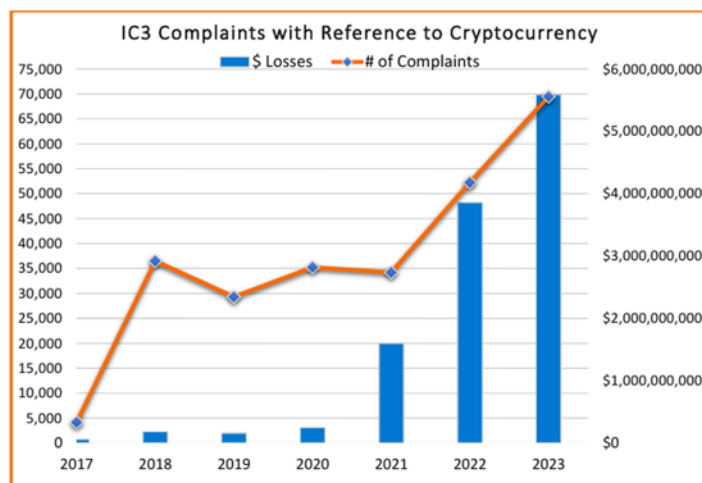
Crypto Enables Fraud

The latest data show that in 2023, the FBI's Internet Crime Complaint Center ("IC3") received more than 69,000 complaints regarding financial fraud involving crypto. Estimated losses from crypto frauds were \$5.6 billion. Perhaps most troubling is that the FBI's report reveals that crypto frauds are becoming more prevalent and costly (see Chart 3). Losses from crypto fraud now account for nearly half of total losses from all types of fraud.³⁵

³⁴ FEDERAL DEPOSIT INSURANCE CORPORATION, *supra* note 7, at 13-15.

³⁵ FEDERAL BUREAU OF INVESTIGATION, *supra* note 9, at 5.

Chart 3



Crypto Harms Minorities and Underserved Communities

Crypto claims that it is an innovative financial product that can be highly beneficial to those who have been shut out of, exploited by, or discriminated against by the traditional banking and financial systems. These claims are targeted at the unbanked, the underbanked, low- and moderate-income households, and communities of color, particularly Black Americans (as well as targeted at policymakers and elected officials who care about such people).³⁶ Financial inclusion and wealth creation are the core of crypto's claims and marketing. Advocates, including some prominent figures,³⁷ often promote crypto as a tool that could reshape, if not displace, the traditional financial system.

³⁶ Dennis Kelleher & Cantrell Dumas, *Crypto's Predatory Targeting of Minority Communities*, Better Markets (Oct. 24, 2024), https://bettermarkets.org/wp-content/uploads/2024/10/Better_Markets_Fact_Sheet_Crypto_Impact_Minorities-10.24.24.pdf.

³⁷ FinTech Global, *From fame to FinTech: ten celebrity-backed financial firms you must know about* (July 7, 2021), <https://fintech.global/2021/07/07/from-fame-to-fintech-ten-celebrity-backed-financial-firms-you-must-know-about/>.

One of the most significant reasons for crypto’s appeal to minority communities, especially, is the deep mistrust many have toward traditional financial systems.³⁸ Historically, minority groups in the U.S.—particularly Black and Latino communities—have been subjected to financial discrimination, exclusion, and exploitation through practices like redlining, loan denials, predatory lending, and “banking while Black” practices.³⁹ These experiences have rightly generated deep skepticism about the established financial sector, which makes crypto’s promise of an inclusive, decentralized alternative more attractive.⁴⁰ The appeal rests on the idea that anyone, regardless of background, race, ethnicity, and current income level, can access wealth-building opportunities without gatekeepers or intermediaries. As the crypto industry is well aware, this message can be incredibly enticing in communities that have faced systemic exclusion from wealth and wealth-building opportunities. That’s why crypto proponents frequently cite its potential to integrate the underbanked and unbanked into a new financial system without a long disreputable history, providing opportunities that traditional institutions have often denied them.⁴¹

Illustrating all this is the crypto industry’s targeting of minorities with Bitcoin ATMs (“BTMs”) (see Chart 4).⁴² As Bloomberg detailed,⁴³ BTMs have clustered in Latino, Black, and low-income neighborhoods, much like payday lenders and check cashing services. The placement of Bitcoin ATMs suggests ethnic targeting.

³⁸ Silvia Foster-Frau, *Locked out of traditional financial industry, more people of color are turning to cryptocurrency*, THE WASHINGTON POST (Dec. 1, 2021), https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html.

³⁹ See, e.g., Emily Flitter, *The White Wall* (2022); Emily Flitter, *‘Banking While Black’: How Cashing a Check Can Be a Minefield*, THE N.Y. TIMES (June 18, 2020), <https://www.nytimes.com/2020/06/18/business/banks-black-customers-racism.html>.

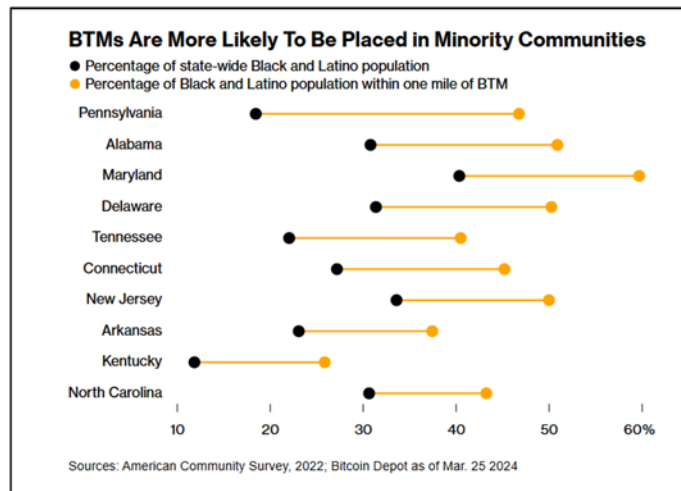
⁴⁰ PYMNTS, *Will 2024 See Crypto Make Good on Its Financial Inclusion Promise?* (Jan. 4, 2024), <https://www.pymnts.com/news/financial-inclusion/2024/will-2024-see-crypto-make-good-on-its-financial-inclusion-promise/>.

⁴¹ COINBASE, COINBASE PRESENTS: BLACK AMERICANS & CRYPTO, <https://www.coinbase.com/learn/community/black-americans-and-crypto> (last accessed Feb. 4, 2025).

⁴² Elijah Nicholson-Messmer & Ella Ceron, *Bitcoin ATMs Flood Black, Latino Areas, Charging Fees up to 22%*, BLOOMBERG (Apr. 17, 2024), <https://www.bloomberg.com/news/articles/2024-04-17/bitcoin-atms-flood-black-latino-areas-charging-fees-up-to-22>.

⁴³ *Id.*

Chart 4



Crypto Is Not Protected by FDIC Deposit Insurance

For nearly a century, FDIC deposit insurance has been trusted by Main Street Americans, who have not lost a penny of insured funds since the FDIC was created. In recent years, though, **crypto firms and other** fintech companies have endangered this trust by claiming that funds customers place with them are also FDIC insured, when in fact they are not.

Since 2022, the FDIC has sent 22 advisory letters to fintech companies, demanding that they cease making false and misleading statements about deposit insurance.⁴⁴ Details differ across the letters, but frequently recurring themes include language implying or flatly stating—falsely—that the fintech itself is FDIC insured, that the fintech customer’s funds are protected by the FDIC in the event the fintech fails, or that crypto assets or stocks are protected by FDIC insurance. ***One entity went so far as to register the Internet domain name “FDICCrypto.com,” where users were redirected to a crypto trading platform.*** A few of the FDIC letters were not sent to fintechs but to fintech or crypto trade publications that ran advertisements stating that various fintechs were FDIC-insured. Despite their tough wording, the FDIC letters were not binding orders; instead, the letters were only warnings that if the misconduct did not stop, the FDIC could, at some point, exercise its authority to

⁴⁴ Better Markets Comment Letter, *supra* note 5.

take formal enforcement actions. Inexplicably, the FDIC has not publicly used its authority to address this misconduct by holding either the fintechs or their partner banks formally accountable.

The bottom line is that these egregious misrepresentations by crypto firms deceive customers and severely harm them financially.

Regulatory Responsibilities

As detailed earlier, banking regulators have clear goals and legal mandates that apply to all business decisions made by banks, whether or not they involve crypto companies. These include promoting access to banking services, ensuring compliance with law, and operating banks in a safe and sound manner.

Existing Risk Management Principles

The banking agencies have made several clear statements that reinforce this approach. For example, in 2015 the regulators said:

Financial institutions that can properly manage customer relationships and effectively mitigate risks are neither prohibited nor discouraged from providing services to any category of customer accounts or individual customer operating in compliance with applicable state and federal law.⁴⁵

In 2023, specifically in response to concerns about crypto companies, the banking regulators issued a joint statement confirming that banks should apply existing and appropriate risk management principles to crypto-related entities, and:

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.⁴⁶

Regulators go further and describe steps that may be effective for banks when assessing and managing the risk of crypto entities, including:

- 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.

⁴⁵ Federal Deposit Insurance Corporation, *Statement on Providing Banking Services* (Jan. 28, 2015), <https://www.fdic.gov/news/financial-institution-letters/2015/fil15005.html>.

⁴⁶ Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, & Office of the Comptroller of the Currency, *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities* (Feb. 23, 2023), <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230223a1.pdf>.

- 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.
- 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.⁴⁷

Bank Secrecy Act

Banking regulators also apply a series of laws and regulations known as the Bank Secrecy Act (“BSA”) to combat money laundering and the financing of terrorism. A representative description of banking agency policies toward BSA enforcement is as follows:

The FDIC and the other federal banking agencies recognize that as a practical matter, it is not possible for a financial institution to detect and report all potentially illicit transactions that flow through an institution. Isolated or technical violations, which are limited instances of noncompliance with the BSA that occur within an otherwise adequate system of policies, procedures, and processes, generally do not prompt serious regulatory concern or reflect negatively on management’s supervision or commitment to BSA compliance.⁴⁸

Concerns about debanking have been expressed in the context of the BSA. For example, a banking industry trade group recently argued that:

[B]anks are heavily incentivized to file SARs [Suspicious Activity Reports] because even an isolated and inadvertent miss can give examiners a reason to sanction a bank or call its entire risk management system into question,”

⁴⁷ *Id.*

⁴⁸ Federal Deposit Insurance Corporation, *Statement on Providing Banking Services* (Jan. 28, 2015), <https://www.fdic.gov/news/financial-institution-letters/2015/fil15005.html>.

and that in turn, examiners will expect banks to close an account for which there are frequent SARs.⁴⁹

This assertion is misguided and wrong. ***The public record of enforcement actions listed on agency websites is consistent with actions taken to address apparent violations of law and to address unsafe and unsound practices, on a fact-specific and well-supported basis, at specific banks.*** Federal banking agencies' actual enforcement actions related to the BSA cite serious and sustained programmatic shortcomings in BSA compliance.⁵⁰ ***Any shortcomings in the banking agencies' enforcement programs, rather, are in the direction of being insufficiently forceful to appropriately protect the public.***

Bank-Fintech Partnerships with Crypto Firms & Related Deposit Insurance Concerns

Banks are increasingly entering into partnering relationships with fintech firms, including some crypto firms, to provide financial services to customers. In these arrangements, the bank remains responsible for ensuring that activities conducted by its partner on its behalf comply with applicable law. Consistent with this principle, the banking agencies have issued several enforcement actions against banks for legal violations attributable to their fintech partners.⁵¹

In addition to these formal actions, the FDIC has issued numerous warning letters over the last few years in response to false statements made by fintech firms about the applicability of deposit insurance coverage.⁵² Frequently recurring claims made by the fintech firms—all false—are that the fintech firm is FDIC-insured, that cryptocurrency is FDIC insured, or that the FDIC will protect fintech customers if the fintech fails.

Better Markets has observed that the FDIC's response to these false claims has consisted solely of letters to the fintech firms warning them that formal penalties could be applied if the conduct does not stop. We have been unable to identify any formal actions penalizing these false statements against culpable fintechs, or their partner banks. The lack of formal penalties for this egregious misconduct, which has deceived and financially

⁴⁹ Bank Policy Institute Staff, *The Truth About Account Closures* (Dec. 13, 2024), <https://bpi.com/the-truth-about-account-closures/>.

⁵⁰ This statement is based on an informal review of the 29 enforcement actions cited in Better Markets' Comment Letter, *supra* note 5, and informal review of high-profile regulatory BSA enforcement actions involving large U.S. banks.

⁵¹ Informal review of 29 enforcement actions listed in Better Markets, *supra* note 5.

⁵² *Id.* at 8.

harmed tens of thousands of ordinary citizens, is a regulatory failure and a disservice to the public.

Recommendations

In conclusion, Better Markets believes that banks should take a risk-based approach to assessing individual customer relationships. If a bank enters the relationship, any resulting violations of law or unsafe and unsound practices can and should be vigorously addressed by the regulators. While the banking regulators' actions and overall approach to crypto entities have been consistent with their duties to enforce the law and protect the banking system, there are several opportunities to improve the clarity of expectations of banks.

More Clarity on the Rules and Expectations of Banks

As detailed earlier in this document, the banking regulators have issued multiple statements on expectations for banks that are providing services to crypto entities. These could be further clarified with more detailed direction or as former Consumer Financial Protection Bureau ("CFPB") Director Rohit Chopra described as "objective, quantitative, and individualized" risk assessments.⁵³ Chopra, who proved that government can work for the American people by returning \$6.5 billion to consumers who were ripped off by the financial industry's greed and unlawful actions since 2021, rightly said that more bright-line limits could help to combat inappropriate instances of debanking.

Greater Disclosure Requirements for Banks

Chopra also recommended increased transparency to combat the perception of arbitrary debanking activity. The current banking rules put limits on the amount of information on the reasons for a bank account closure that can be shared publicly. If banks were required to specify the reason for an account closure, however, there would be less chance of misunderstanding or jumping to conclusions about malicious intent or discrimination when an account is closed.

⁵³ Jon Hill, *CFPB's Chopra Sees Room For Rules To Stem Debanking*, Law360 (Jan. 27, 2025), <https://www.law360.com/articles/2289603/cfpb-s-chopra-sees-room-for-rules-to-stem-debanking>.

Chairman MEUSER. Thank you.

Now, I would now like to explain how Ranking Member Green and I have agreed to establish the question order. We will follow the rules of the committee alternating between one Republican and one Democrat member for 5 minutes each, with the exception that Mr. Green will be the last Democrat member to speak or to ask questions immediately before the last Republican member.

We will now turn to member questions. The chair, myself—I will recognize myself for 5 minutes.

Mr. Campbell, so you witnessed firsthand how Operation Choke Point was orchestrated in the past. Can you give us some details, walk us through the specific directives or tactics regulators used back then, which pressured banks into severing ties with legally operating businesses, and how those tactics have sadly been recognized in the more recent past related to crypto?

Mr. CAMPBELL. Yes, sir. Of course. I would say, when you are in a risk officer position at a bank, as I have been in the past, and you are communicating with regulators, you are getting fundamentally several layers of guidance from them. One is whatever the written findings are that they eventually come to the conclusion of examination or something of that sort, but through the course of that and prior to the written findings is a lot of verbal guidance.

When you were attempting to engage in certain types of crypto activities, the kinds of statements you would get, which you will see banking regulators making to this day in public, in fact, Jerome Powell, Chairman of the Federal Reserve, said similar things recently is: While you are not legally prohibited from doing these things, we find them to be extremely risky, and there is no particularized analysis of why they are risky, right.

If you were to say, well, you have told me giving a deposit account to a crypto company is risky because maybe these deposits will flee quickly, and you say something like, okay, I hear you, I will segment those deposits and back them only with T-bills, the safest, most liquid asset known to man in the world, essentially unlevered, no long-dated lending. They say, well, we have reputational concerns about you banking crypto clients. We are still not sure. Maybe we will answer you on that, maybe we do not, but we still find it risky. You understand that to mean, no, right. I am a parent. I have two kids. They understand when they ask me if they want to do something or not and I say, well, you can do what you want, but I would not if I were you. They know that really means, no. One thing they do is this.

The other thing they do which, Paul, you had referenced this earlier that the pause letters and sort that recently came out from the FDIC indicate, is they will just ask you questions endlessly and tell you that you need to get permission from the regulator to engage in these activities and hopefully they will never stop asking questions, right. This could be 2 years straight of questions with no end point, no finish line, no clear articulation as to what they are trying to learn. At some point, it just becomes a repetitive cycle, and it is clear the answer is no.

The final point is, as I said with the regulatory guidance, they will start punishing you in other ways. They will look at your business and start tweaking your CAMELS ratings, they will start rais-

ing the operational risk of your bank, they will start downgrading your management judgment because you have persisted in offering these sorts of concerns. They will even go so far, in many cases, as to pressure banks providing you with services, if you are a small bank, to stop doing so.

For instance, there have been cases of smaller banks having their corresponding banking relationships terminated so they can no longer send international wires or things of that sort where regulators went and pressured other people serving them.

Chairman MEUSER. All this is quite damaging.

Mr. CAMPBELL. Those are extremely damaging, and I would tell you; these efforts make it uneconomic to serve the crypto industry. While there is no legal ban, there is a functional ban for a for-profit institute approaching this space—

Chairman MEUSER. All right. Thank you.

Mr. CAMPBELL. Thank you.

Chairman MEUSER. Mr. Grewal, thank you. The significance of these pause letters, can you kind of summarize that for us?

Mr. GREWAL. Yes, sir. What the pause letters show, Chairman Meuser, is that over and over again, banks were subject not to regulation by examination, but regulation by exhaustion. You had question after question raised if even a hint of interest was shared that the bank wanted to enter into a basic service for its customers involving crypto or to facilitate basic crypto transactions.

What makes the pause letters particularly troubling is that all of this activity, all of this exhaustion and re-and re-examination took place against a backdrop of the FDIC telling the public something very different. This comes in the form of the response to the inspector general report that I have referenced in my opening statement.

It was in that response that the FDIC suggested that banks had every right to participate in crypto activity. We know that was false, and we know that they had no intention of ever permitting that activity to take place. It is that practice of saying one thing in public and doing something very different in private that I think is particularly concerning, and it is something that this committee ought to pay attention to.

Chairman MEUSER. Right. Thank you.

Mr. Thiel, in spite of the actions taken by the FDIC, which were egregious and somewhat astonishing, the damage caused, are there solutions, and are those solutions quite attainable?

My time has expired, so I would like to hear that answer throughout the course of this testimony. Thank you.

I now yield to the gentlewoman from California, Ms. Waters, ranking member of the full committee, for 5 minutes for questions.

Chairwoman WATERS. Thank you very much, Mr. Chairman.

While I would like to really engage on this question of debanking, having worked on stablecoins and understand what is going on, both with the big banks of America and with crypto, let me just say, the big banks are not interested in opening up banks to the small people, to poor people, and they have debanked large segments of the communities of America already.

With crypto, they are divided. Crypto talks about, some of them want regulations, others do not want regulations, so I am not going

to spend my time talking about them. This fight is going to go on for quite some time. We must, however, acknowledge the takeover of the Federal payment system by an unelected billionaire donor that took place last week.

Despite resistance from senior officials, Co-President Musk seized access to Treasury payment systems, including the sensitive, personal data of virtually every American. I have heard from hundreds of people who are worried about Elon Musk having access to their sensitive data, including the impact on Social Security payments and Medicare benefits. What are the implications of this illegal takeover for the American people?

While we have been confronted with chaos in the past few days, and we are trying to figure out what is going to happen to those employees, those Federal Government employees have been told that they are going to be furloughed. They do not know what is going to happen to them. I was absolutely shocked that when the President of the United States said to all of the departments that supposedly have people that are working in diversity, equity, and inclusion, out by 5 o'clock. It sounded to me like some of those times that we witnessed in the past with communities that told people to be out by sundown, et cetera, et cetera.

We can talk about what is going on with debanking all that we want, but America is in trouble, deep trouble. It is not simply about what is happening here with the leadership of this government in America. They are all over the country. I just discovered that Elon Musk is threatening the President of South Africa. We worked very hard dealing with South Africa and getting rid of the kind of racism that was involved historically. Now they are being threatened because Elon Musk is going to open up a battery factory in South Africa. He wants them to get rid of the 30 percent participation that was fought for so that Black South Africans could participate.

Trump is saying to the South African Government, if you do not get rid of your diversity, equity, and inclusion, we are going to cut-off all of the support through the U.S. Agency for International Development (USAID). USAID has been shut down, and it was shut down by the Co-President Elon Musk. Guess why? He is under investigation by the USAID.

While we talk about debanking, that is an issue, and I am going to tell you, the banks and crypto are going to fight it out. I guess the biggest billionaires will win, because that is what it seems to be all about in this country these days, and that is about billionaires and their power. Go on and talk about it, but I am going to fight for the opportunity for the average person in this country, for the little people to have some kind of banking services. We have been screaming about payday loans. We have been screaming about a lack of access for people in poor communities. That is not a big issue anymore. It is about whether the big banks and crypto are going to find a way to get along.

You all carry on with this today, but I want you to know, I am going to continue to pay attention to what the Co-President is doing, what this President is doing, and the kind of rally that we are seeing over at the Treasury Department just a day ago, where everybody came together, thousands of people, to say hands off our

private information, hands off Social Security, hands off what is happening with the tax revenue in this country.

With that, I know you are glad. I yield back the balance of my time.

Chairman MEUSER. The gentlelady yields.

Without objection, I ask unanimous consent to enter into the record the statement by the Department of Treasury about what is actually happening within the payments system and the level of security that has been assured by the Secretary of the Treasury.

Without objection.

[The information referred to can be found in the appendix.]

Chairman MEUSER. We now recognize the gentlewoman from Missouri, Mrs. Wagner, who is also the Chair of the Subcommittee on Capital Markets, and now recognized for 5 minutes.

Mrs. WAGNER. I thank you, Mr. Chairman, and congratulations on your new gavel.

I am going to try and turn us back to the topic of the day, and I thank our witnesses for sharing the difficulties their firms have had accessing routine banking services simply because of their involvement in the digital asset ecosystem.

It is clear that under the previous administration, the Biden Administration, digital asset firms were the victims of a pressure campaign initiated by regulators, designed to cut them off from our economy. Regulators should not be picking winners and losers based on what industries enjoy, the political favor of the sitting President. Individuals operating fully legal businesses deserve their right to seek access to banking, and banks must be free to make decisions about the customers they serve without regulators pressuring them to toe the hostile administration's line.

Mr. Thiel, has your bank ever stated whether their prudential regulators told them that they should refrain from providing services to digital asset firms?

Mr. THIEL. Representative Wagner, we banked with Signature and when the FDIC shut them down and Flagstar took over the accounts, none of the crypto accounts were allowed to be part of those assets acquired, and we were forced to immediately seek accounts with other banks. We were able to open an account with another bank, deposited \$70 million after going through all the approval processes, and 6 days later, we were told we have to shut down the accounts because our bank no longer will bank crypto companies.

Mrs. WAGNER. The answer is, yes?

Mr. THIEL. Yes.

Mrs. WAGNER. What did they say?

Mr. THIEL. We were basically given a policy decision by the bank that they would no longer service crypto companies, period, and we were asked to withdraw our money in, I think it was, 24 hours or 72 hours.

Mrs. WAGNER. No explanation, just by fiat?

Mr. THIEL. Yes.

Mrs. WAGNER. Wow.

Mr. Campbell, do you believe the treatment by the prudential regulators related to digital assets differs from the treatment of other lines of business transactions and portfolios?

Mr. CAMPBELL. I definitely do. There was actually a study recently by the Alternative Investment Management Association (AIMA) and John D'Agostino that I reference in my written testimony, where they went and systematically surveyed asset management firms, those who were traditional asset managers, so call it the fidelities of the world and hedge funds and things of that sort, and then those that served crypto.

Among the traditional asset managers, many of whom do engage in highly risky strategies, and I say this as somebody who has worked at a traditional asset manager myself, almost none of them had problems accessing banking service, but among the crypto segment, even those doing the most vanilla, most boring, long-only sort of strategies, roughly two-thirds had problems acquiring banking services.

Mrs. WAGNER. Wow.

Mr. CAMPBELL. There was a large disparity.

Mrs. WAGNER. I would like you to get me that study, and we will submit it for the record. Thank you.

[The information referred to was not received prior to printing.]

Mr. Campbell, do you believe that regulators are using debanking as a tool to advance their anti-digital asset agenda?

Mr. CAMPBELL. I do, and you see this in many of the FDIC pause letters where they just say crypto is bad, and you ask them, why do you think crypto is bad? They say, because it is risky. You ask them, why do you think it is risky? They say, because it is bad, right. It is circular reasoning, and they never really give any fundamental justification for why it might be risky for, say, Mr. Thiel's company to make payroll, right, or pay their rent. That is sort of what gives lie to me of the behaviors, the inability to provide even basically riskless banking services.

Mrs. WAGNER. Okay. We have also seen overzealous regulation by enforcement—and that is what I call it, regulation by enforcement—by the SEC. Mr. Grewal, how has the regulation by enforcement approach hurt U.S. leadership in technology and financial innovation?

Mr. GREWAL. Congresswoman, respectfully, I think another way to ask that question maybe, how has it not hurt us to be sued by the SEC after years of asking, indeed begging, for simple rules from the Securities and Exchange Commission—

Mrs. WAGNER. I know.

Mr. GREWAL [continuing]. that could be followed and allow companies like ours to accept their invitation to come in and register.

Mrs. WAGNER. Would you clarify a little bit more, can you describe Coinbase's efforts to gain clarity from these regulators and financial institutions?

Mr. GREWAL. Yes. Yes, ma'am. We have formally requested rules by petition. That petition was denied by the SEC. That denial was found to be arbitrary, capricious, and the reasoning vacuous by the U.S. Court of Appeals. We have attempted to meet with the SEC on dozens and dozens of occasions with our own ideas for how regulation might work, and what standards might apply to the industry as a whole. Over and over again, we were thwarted. We were told, thank you and go away.

Mrs. WAGNER. Thank you. I am sorry. We are going to get this straightened out.

My time has expired. Mr. Chairman, I yield.

Chairman MEUSER. The gentlelady yields.

The chair now recognizes the gentlewoman from Michigan, Ms. Tlaib, for 5 minutes.

Ms. TLAIB. Thank you, Mr. Chair.

Ms. Olesiuk, what would you say to a family member, that a friend that came up to you super excited to invest in crypto or digital assets? I think we all had that one cousin that called. What would you say to them before they invested?

Ms. OLESIUK. Thank you for the question, Congresswoman. I think that Americans are skeptical of crypto, and rightly so. Americans have seen the illegal activity, arrests and just dangerous activity. Looking at a Consumer News and Business Channel (CNBC) poll, only 8 percent of Americans have a positive view of crypto. Looking at the Federal Reserve data, only 7 percent of Americans own crypto, and only 1 percent use it to buy things, so I would encourage them to have some caution and to—encourage them to go to a traditional bank where—

Ms. TLAIB. Yes. I raise the question because there are Detroit residents who have lost thousands of dollars of cryptocurrency in my district. I actually have—one of my Livonia residents right outside of the city recently contacted our office where she had lost \$400,000 through a cryptocurrency scam, and it was just heart-breaking. I just feel like we cannot—we cannot ignore that.

Today's hearing, of course, is supposed to be about debanking faced by the crypto industry, but if we really were concerned about financial inclusion, we know that many of the most vulnerable among us, Black, Brown, low-income, lack access to basic financial services. I know across the country we have charities, individuals, and businesses experienced trouble opening a bank, maintaining their account, sending or receiving payments because of religious or ethnic national affiliations.

I say this because, as one of the only few Muslim Americans serving in Congress, I was surprised to see that one of the polls found—one of these polls found that more than one out of four Muslim Americans reported challenges while banking. Someone said in my district once, it is called banking while Muslim, right.

Ms. Olesiuk, how can lawmakers be able to combat such discriminatory debanking practices?

Ms. OLESIUK. I think I would answer with two things. First, to strengthen oversight and increase accountability to ensure that banks are following the appropriate laws and regulations that—anti-discrimination laws that protect all Americans. Secondly, under the former Consumer Financial Protection Bureau (CFPB), Chair, Director, I think some good work was being done to explore alternative methodologies for people without credit to build credit.

Ms. TLAIB. Yes. I think this is more because they are Muslim.

Now, I would like to discuss facts motivating today's hearing, and Coinbase's—and it is a consultant's complaint against the FDIC. They claim, they quote, starting—you are probably familiar with this—Starting in 2022, Federal financial regulators have taken concerted steps designed to cripple the digital asset industry.

What is interesting about this timeline—and maybe, Ranking Member, you would find this interesting—what actually happened around 2022? Folks are forgetting. They were going to play dumb, but we were not. We know what happened. Investors lost \$2 trillion during what we call, what, crypto winter, and a whole host of crypto and digital asset companies went belly up, including FTX and Celsius.

In early 2023, we saw Silicon Valley Bank, Signature Bank and Silvergate fail with crypto playing a huge role in that. How would you characterize the crypto industry's access to banking services before crypto at companies and regional banking failures around 2022?

Ms. OLESIUUK. I think that the—there was caution and the regulators recognizing the risk that these companies—

Ms. TLAIB. They messed up, right? They messed up. They failed. That is \$2 trillion.

Ms. OLESIUUK. True.

Ms. TLAIB. Yes, but they act like, poof, we were just like picking on them.

Ms. OLESIUUK. True. I—

Ms. TLAIB. We were picking on them. They messed up.

Ms. OLESIUUK. The regulators and banking regulators recognized the risk that these companies presented and then we saw what happened in 2023.

Ms. TLAIB. Yes. Really quick, I know according to the FDIC's inspector general reported in early 2023 that 136 FDIC-insured banks have ongoing or planned digital asset activities. It sounds like crypto industry was doing okay in term of access. Then the industry tanked, banks got spooked, and regulators took a closer look.

Would you agree with this rough timeline and description? I think it is important for American people to understand this, as we sit here. What happened before all of a sudden you guys all got the knock on the door? Something was happening, and so, I think it is really important. Again, it is the regulators got tougher after multiple bankruptcies and related bank failures. That is a fact, and it is part of the, again, I think the facts that nobody is going to bring up. You fail; you are hurting American people. We are going to have oversight, and we are going to make sure it does not happen again. Thank you.

Chairman MEUSER. The gentlelady yields.

Mr. Loudermilk of Georgia is now recognized for 5 minutes for his questions.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

I thank the panel for being here. It is a very important topic, and it is something that has to be addressed. With the original Choke Point, Federal regulators carried out a coordinated campaign of harassment against law-abiding businesses based on thinly defined reputational and regulatory risk. That resulted in the systemic debanking of thousands of American businesses, legal businesses, and I would argue constitutionally protected businesses, like gun dealers, pawn shops, and installment lenders. While the first Trump Administration ended this abuse of regulatory power, the

Biden Administration regulators wasted no time in bringing it back with a new target, innovators and entrepreneurs.

My first question, Mr. Campbell. To carry out their politically motivated campaign against American innovation, Biden regulators use something called supervisory non-objection letters. Can you briefly explain what these letters are and what they meant for banks?

Mr. CAMPBELL. Yes, of course. It basically requires a bank to go to a regulator and get non-objection, that is to say they do not tell you no, to be allowed to engage in any sort of banking activity.

Mr. LOUDERMILK. In your opinion, do these letters change the law as enacted by Congress?

Mr. CAMPBELL. I think when they are abused there is that potential, yes. In fact, to the previous representative's point, we are somewhat twisted around here in that the regulators took the stance of, because some actors in a space are bad, we will therefore debank all of the actors in a space. Which you will notice is the exact sort of the line of thinking that has been promulgated to justify the actions of the FDIC with regard to Choke Point, but also, was the rationale behind red lining and the denial of banking services to minorities in the past. I would suggest it is a governance issue, yes, sir.

Mr. LOUDERMILK. All right. Thank you for that.

The Trump Administration regulators, particularly the OCC also used supervisory interpretive letters during his first term. What are the main differences between those interpretive letters and the supervisory non-objection letters issued under the Biden Administration?

Mr. CAMPBELL. Interpretive letters are attempting to parse through the law and give people a path to either engage in actions or a rationale not to engage in those actions, hopefully well-founded. When they are made public, I think they are very valuable, because then everybody is playing by the same rule set. The non-objection letters were particularized, individual, and private. Exactly as Mr. Grewal said earlier, there is no way to know what each individual bank is being told, and it allows a regulator to say one thing publicly and do something else privately, or just as bad, favor some banks over others.

Mr. LOUDERMILK. I guess the title of the letters is definitive interpretive versus non-objectional, okay. Thank you for that.

Mr. Grewal, did the Biden Administration specifically issue the supervisory non-objection letters to target digital assets that were previously allowed by the Trump Administration?

Mr. GREWAL. Yes.

Mr. LOUDERMILK. If banks must ask regulators for explicit permission to bank crypto firms, how does this affect their willingness to bank those firms?

Mr. GREWAL. It discourages those banks from even trying in the first place, Congressman. The reason is that having to submit those requests under a well-defined framework with a deadline is one thing, but to simply submit and wait for an answer whenever and according to whatever standard the regulator deems fit, that is something else entirely, and that is something that ultimately discourages banks from even participating in the first place.

Mr. LOUDERMILK. Sir, are you aware of any banks that went through the non-objection process, and if so, how did those banks fair?

Mr. GREWAL. I am aware of my examples of banks who went through that process as a result of the documents that we secured through our FOIA suit against the FDIC. What we saw in the documents that were produced just yesterday is that in case after case when the banks step forward and raise their hands and ask for permission to offer basic services, they were either ignored or they were given detailed examination and re-examination and re-, re-examination until they simply gave up.

Mr. LOUDERMILK. There was a time, and I believe that the administrative state was established to work with industry to provide guidance, create some consumer protection. I remember when FDIC was viewed as a partner with banks, it would help the banks to operate in a functional. This sounds to me like this is an adversarial relationship instead of a partnership. Would you agree with that?

Mr. GREWAL. I would. If there was an offer made, it was an offer that the banks were not allowed to refuse.

Mr. LOUDERMILK. Thank you. I yield back.

Chairman MEUSER. The gentleman yields.

The chair now recognizes the gentlelady from Georgia, Ms. Williams, for 5 minutes for her questions.

Ms. WILLIAMS of Georgia. Thank you, Chairman Meuser and Ranking Member Green.

Now, colleagues, I am going to need a little help from you all in this first portion.

Raise your hand if you have been overloaded this week with urgent calls from constituents worried about how President Biden treated crypto firms.

Okay. I did not get any calls about this this week. No.

Raise your hand if you have gotten urgent calls from your constituents about an unelected billionaire and his overreach in the agencies that this committee oversees and harming those most marginalized.

My phones have been ringing off the hook.

Exactly what I thought. My colleagues are saying the same thing.

You all, this is our first subcommittee hearing, and it is going to be about fake oversight over the crypto policy of former President Biden. He is not even in power anymore.

Are we really going to ignore all of our constituents who have reached out with their frustrations, confusion, and concerns about Elon Musk dismantling our Federal Government? Getting answers for our constituents is what this subcommittee should be doing.

Now, look, I fully understand the importance of the crypto industry. The digital asset market is rapidly growing throughout my district, especially in my home city of Atlanta. I get it, you all. I want my people to thrive. The Financial Services Committee should have serious bipartisan conversations about crypto policy but saying that President Biden's policies discriminated against crypto firms is not a serious take. It is a distraction from the mess that my colleagues—my Republican colleagues are creating here in D.C.

I have a better idea. If my Republican colleagues want to talk about discrimination in the banking system, let us have a real conversation about that and I will start.

Ms. Olesiuk, the city of Atlanta has one of the largest racial wealth gaps in the country. Did that just emerge over the last 4 years because of President Biden's so-called discrimination against cryptocurrency?

Ms. OLESIUK. Thank you for the question, Congresswoman.

No, the wealth gap has actually been growing for years and decades now and has actually gotten worse, not better.

Ms. WILLIAMS of Georgia. Exactly. I did not think so.

Ms. Olesiuk, let me try another theory. Did the racial wealth gap emerge in part because of the long legacy of discrimination against Black and Brown Americans in the banking system?

Ms. OLESIUK. Yes, I believe that has contributed. Black and Brown Americans do not feel comfortable going to traditional banks, often. They feel discriminated against so, yes, I believe that is a major contributor.

Ms. WILLIAMS of Georgia. Now we are getting somewhere.

Many Black and Brown Americans have been historically turned away from the traditional banking system simply because of the color of their skin. Many Black entrepreneurs still have cash-only businesses.

Ms. Olesiuk, what can regulators do to address the real needs of unbanked individuals like so many throughout my district in Atlanta?

Ms. OLESIUK. I think this is a key question, and I have a couple of suggestions.

First of all, there are what are called Minority Depository Institutions, or MDIs. These are banks that are specifically focused on serving minority communities. There have been many studies that show that Black and Brown people who go into a bank where they see people that they feel comfortable with, they often—loan approvals are better, and they have a better experience at a bank. So, encouraging more of the MDIs to open. Unfortunately, they are on a downward trend now, so that is something that we need to do.

Also, expand diversity in public and private leadership, both at banks and at the agencies, to ensure that the policies are serving everyone.

Ms. WILLIAMS of Georgia. While my Republican colleagues want to discuss getting bank accounts for cryptocurrency, I want fair policies. I want it across the board, but I wonder more about getting bank accounts for the people in my district who remain unbanked. I was once unbanked myself. Unfortunately, recent data shows that 11 percent of Black American households are still unbanked, compared to 2 percent of White households.

Ms. Olesiuk, will attacking and getting rid of diversity, equity, and inclusion programs throughout the government help close the racial wealth gap or widen this divide?

Ms. OLESIUK. Oh, it will absolutely widen the divide. It is not going to help at all.

Ms. WILLIAMS of Georgia. Thank you so much for this conversation today.

I hope that we can continue to make sure that, while we are not only looking out to make sure that cryptocurrency firms and everyone who is seeking to thrive in this industry have access to bank accounts, that we are also looking out for those people that we were sent here to serve, like the people in my district in Atlanta.

It is clear that we have a lot of work to do in this Congress, but if we are going to do it, we have to talk about the real problems facing real people.

Thank you, Mr. Chairman, and I yield back.

Chairman MEUSER. The gentlelady yields.

The chair now recognizes Mr. Garbarino from New York for 5 minutes.

Mr. GARBARINO. Thank you, Mr. Chairman.

Thank you to the witnesses, also, for being here today.

One story that we have consistently heard from opponents of digital assets is how it provides a significant source of financing for terrorist groups and other illicit activities.

However, the evidence tells us a different story. According to a recent report, illicit activity is down, with analysts estimating that crypto transaction volume associated with illicit activity is only at 0.34 percent.

Mr. Grewal, how do companies like Coinbase approach Know Your Customer and anti-money-laundering requirements with financial institutions?

Mr. GREWAL. Thank you for the question, Congressman.

Coinbase is licensed in 45 States as a money transmitter, and also the New York BitLicense also applies to our firm. We are a registered money-services business with Financial Crimes Enforcement Network (FinCEN) under the Department of Treasury. We also have broker-dealer licenses all over the Federal Government, as well, at the SEC, and we are also licensed at the Commodities Futures Trading Commission (CFTC).

With respect to your question, we take our obligations to follow the Bank Secrecy Act (BSA) and all Know Your Customer (KYC) and anti-money laundering (AML) rules extremely seriously. We have hundreds of employees and thousands of contractors who work on these issues each and every day.

To the extent you or any other member have questions about the strength of our commitment to law enforcement and enforcement of the Bank Secrecy Act, I encourage you to speak with the men and women of law enforcement at the FBI, the Drug Enforcement Administration (DEA), and across this country in State and local departments. I think they will tell you that their best days are when they are investigating crime that involves cryptocurrency as opposed to cash or other forms of payment that are far more prevalent in this country. They prefer to work with Coinbase.

Mr. GARBARINO. Thank you very much.

Mr. Thiel, prior to being debanked, had you provided all necessary information to your bank in order for them to be compliant with KYC and AML standards?

Mr. THIEL. Yes, sir.

Mr. GARBARINO. Had your previous banking partner raised any KYC or AML concerns with you during that relationship?

Mr. THIEL. None, sir.

Mr. GARBARINO. Since being debanked, do the institutions you attempt to receive service from cite KYC or AML risks associated with your company?

Mr. THIEL. No, sir, Congressman. They essentially just say they have a policy against crypto. In some cases, the KYC process can take years, and then they simply say, "Unfortunately, our committee will not allow a crypto customer."

Mr. GARBARINO. That is because of regulators?

Mr. THIEL. Correct, sir.

Mr. GARBARINO. Yes. You have had no concerns with KYC and AML. Banks do not bring that up to you. They just say they cannot do business with crypto.

Mr. THIEL. Sir, we are a fully SEC-regulated company, audited financials. They do not raise any issues like that.

Mr. GARBARINO. The regulators are the ones who are leaving you where you are right now?

Mr. THIEL. We believe so.

Mr. GARBARINO. Yes. Thank you, and Mr. Campbell, you are familiar with KYC and AML requirements, correct?

Mr. CAMPBELL. Yes, sir.

Mr. GARBARINO. Can you describe some of the issues that are considered when institutions are working through these requirements?

Mr. CAMPBELL. Yes. You are looking at the legal identity of the customers, the validity of their business activity, the source of funds, the expected activities over time, what you might think of as deviations from that, compliance with law, and so on.

If I was sitting at a bank and evaluating, say, Coinbase, I would be looking at things like, are they licensed, what is their staffing, what are their policies, where do they get their money? You are doing a comprehensive analysis of the behavior of a client.

Mr. GARBARINO. Yes, it is a very deep dive, and you feel comfortable after doing it.

Mr. CAMPBELL. Hopefully you do.

Mr. GARBARINO. You would want to, at least.

Mr. CAMPBELL. Yes. Look—and when you do not, usually you should have found something particular, like, oh, this owner is on an Office of Foreign Assets Control (OFAC) sanctions list, or, oh, they appear to be laundering money for X, Y, Z reasons. It is not really supposed to be about, for lack of a better word, vibes.

Mr. GARBARINO. Yes. I appreciate that and I appreciate all the witnesses with your answers here. It is obvious that the regulators are—it seems that they are the real reason that you are all here today testifying and not the banks. We have to get that under control. That is our job here at Congress.

I appreciate you all being here, and I appreciate the chairman for having this hearing, and I yield back.

Chairman MEUSER. The gentleman yields.

Mr. Liccardo of California is now recognized for 5 minutes.

Mr. LICCARDO. Thank you, Mr. Chair.

Thank you to all the witnesses for your statements.

I appreciate my colleague Congresswoman Williams' frustration with the focus of the subcommittee on a historic analysis of regulation, which—I think I might agree with many of the assertions

made that in some cases may have been an overreach. In other cases, I do not think so, but regardless, his administration is no longer in office. I would much rather focus on a forward-looking approach of what we can do to make things better. I think debanking and access to banking services is a serious concern.

I hope, Mr. Chairman, that all of us will agree that we need a strong Consumer Financial Protection Bureau to ensure that access to banking services is widely available, in addition to addressing concerns about banking regulators and its impact on debanking. We have about 5.6 million low-income households that critically need access to banking services and are not getting them, so I hope we can be more forward-looking going forward.

On that note, I would like to consider the larger questions that Mr. Campbell raised about banking regulation generally. I thought those were interesting, and I want to pose the question to Ms.—forgive me—Olesiuk?

Ms. OLESIUK. Yes.

Mr. LICCARDO. Thank you. Thank you for your patience with my pronunciation.

I know you have raised obvious concerns about regulation of banks in the context of a digital asset that may have, for example, high volatility.

Mr. Campbell recommends, though, as we are thinking about banking regulation generally, that regulators, going forward, approach regulation in a way that is—and I am going to summarize here, not perfectly, but—first, that the regulation be written, not oral; that it be public, not secret; that it be explanatory of the rationale used to reach the decision; and there be some, for lack of better term, subject to appeal by a third entity.

I am just curious about, in your view of banking regulation, does that make sense, as we think about how we can do better going forward?

Ms. OLESIUK. Thank you for the question, Congressman.

I actually agree with a lot of those suggestions.

I think we need to start with the perspective that regulators must take a risk-based approach to this issue. Regardless of the industry, crypto or otherwise, regulators must look at what risk that is presenting to an individual bank or to the banking system in general, looking through the lens of financial stability.

With regard to the solutions and a way forward—and I describe this more in my written testimony—I have two main suggestions. First, clarity on rules and expectations for banks. I think that will set a level playing field for everyone involved; secondly, more disclosure requirements for banks. I think this will help—it will help with the clarity, but it will also ensure that if someone, whether they are a crypto customer or a minority customer who is trying to get access to banking, they will understand why they are being told no.

Mr. LICCARDO. Thank you.

I want to go to Mr. Grewal for a moment.

I understand the Federal Trade Commission (FTC) has announced on Wednesday that it would withdraw its current guidance to banks on engaging in crypto-related activities. I know you have urged withdrawal of the OCC interpretive letter, I think it

was 1179, which you found to be inconsistent with prior OCC letters.

To what extent does the FDIC's action address your concerns? Do we still need to withdraw—somehow or another enact legislation that would force the withdrawal of that OCC——

Mr. GREWAL. Thank you, Congressman.

Mr. LICCARDO [continuing]. letter?

Mr. GREWAL. I think the FDIC's announcement was a positive step, but I do not think it goes far enough.

The fact of the matter is that, in response to the inspector general's report, the FDIC committed to conducting risk assessments of the crypto activities that the banks wish to engage in. To date, we have no indication whatsoever that they did any assessment of the risks that they claim were so significant that they could not even allow the banks to participate in those activities at all.

The other thing I would point out is that the FDIC, in response to our requests, abused the "confidential supervisory information" designation to redact page after page of materials in ways that were rejected by a Federal court. That needs to be addressed.

Finally, in response to an order from a Federal district court to produce these pause letters that we were referencing, the FDIC misrepresented that its productions were complete.

I do think there is further work that needs to be done in order to restore public trust in the FDIC, but at a minimum, I do think that the announcement yesterday by the FDIC Acting Chair was a constructive one.

Mr. LICCARDO. Thank you.

Thank you, Mr. Chair. I yield.

Chairman MEUSER. The gentleman yields.

Mr. Har—excuse me—Haridopolos from Florida is now recognized for 5 minutes.

Mr. HARIDOPOLOS. Thank you, Mr. Chairman. I have trouble with that name too. No problem.

Thank you very much for putting this together, Mr. Chairman. This has been very illuminating, especially as a first-year member of the committee. It is very helpful to get us into the history of this, and this has been very helpful to get this going.

In this, my first year in the Congress, we are trying to—I know that Congressman Moore and I, both new to the committee, are trying to kind of get under the hood and understand some of these things. As an outsider, we watched the FTX crisis happen, and I think we are kind of wondering where was the oversight? It is frustrating to see so many folks lose, in many cases, their life savings or significant savings and the total disregard for their capital.

One of the messages you will hear from me consistently not only today but throughout the year is "certainty and stability." To me, that is not only important in business but in life, especially as you try to teach that to your kids.

What is really frustrating is, as I tried to do my homework on this, I watched the videos from years past. Before Mr. Gensler, for example, was actually in the job in the government, his videos showed he was actually positive about the industry, thought it would be something productive and creating—using the blockchain to make sure you had that certainty and understood what was hap-

pening. Yet, in some of the first few days in this committee, we have learned that not only that agency but also the CFPB is doing everything they can to move capital out of our own country and go into places like the United Arab Emirates (UAE) and Singapore. America is the land of opportunity and where capital, I think, can strive best.

With that said, I think I will just ask Mr. Grewal, if you do not mind. I know these are rapid-fire questions—I am going to give you a few minutes to walk me through what you went with. We all saw FTX and the lack of regulation. What did you all try to do, in working with the regulators, to say, we want to be regulated, we want to stabilize this?

If you could walk me through—you have a few minutes? I want to give you that opportunity because, too often, I am watching these early days in Congress; it is, “wham, wham, bam.” I want to hear your, kind of, thoughtful, laid-out answer so people can understand what good companies are trying to do versus some of those bad actors.

Mr. GREWAL. Thank you, Congressman.

I referenced earlier the invitation by the prior SEC Chair to come in and register. This was Mr. Gensler’s constant refrain to cryptocurrency firms like mine that were interested in following the law but looked at the law and could see no legal basis upon which to pursue registration.

Registration is a very important element of any sound oversight and sound regulatory framework and structure for firms not just in our industry but, frankly, in any industry.

Over and over again, when we met with the SEC, as I said, dozens and dozens of times, when we presented ideas for a way for intermediaries like Coinbase to register, a way for issuers of the tokens themselves to submit disclosures that would better inform consumers who purchased these tokens what it is they were buying, when we shared ideas and concepts for ways in which the SEC could coordinate its activities over securities tokens and securities transactions with those of the CFTC, which has authority over non-securities and commodities in particular, we thought we had an opportunity. Yet, after these dozens and dozens of meetings, we were simply invited to stand up, step outside, and never come back.

A short while after that, Congressman, we were hit with a lawsuit. For the last 2-plus years, my company and I have been in Federal district court fighting an enforcement case where there is no allegation of fraud, no allegation of abuse, and we have tried at every turn to simply get rules that we can follow.

Mr. HARIDOPOLOS. Thank you, Mr. Chairman. I yield back.

Chairman MEUSER. The gentleman yields.

The chair now recognizes Mr. Moore of North Carolina for 5 minutes.

Mr. MOORE. Thank you, Mr. Chair, and to our witnesses, thank you for taking time to be here out of your schedules to bring this information before the committee.

Just like Representative Haridopolos—you are right, Chairman, it is a tough name. I had to practice it several times—this has been a new experience. I served in our State legislature in North Caro-

lina, and so coming here and seeing things, it has been eye-opening in a lot of ways.

One of the more eye-opening things that I have seen since arriving here is how—I have seen how some of our friends on the other side of the aisle will try to—I would describe it as “weaponize” the regulatory system to try to simply prevent access to forms of capital.

It strikes me—I did a little research here. The country has roughly, what, 334 million people in it. Most recent data shows, of that, anywhere from 27 to 28 percent of the people in our country either own or use crypto. Based on my—I was a solid C student in math, but based upon that, I think that is around 90 million people in this country who have confidence in crypto.

What it seems has been happening by the previous administration and by the other side is an attempt to try to use the regulatory framework to simply tell those 90 million people that they cannot invest or they cannot own in crypto. I cannot, frankly, think of anything that is more antithetical to a free-enterprise system.

I, first of all, thank those of you who are providing these opportunities for just ordinary consumers to be able to participate in a meaningful way in this new digital marketplace. I think it is—digital currency is—not only is the future; frankly, it is the present, when nearly a third of the people in the country are actively using this.

I certainly do not want to repeat comments that have already been made so well by other members of the committee, but the regulatory framework of trying to add in the pressure to banks to not engage with crypto, the pause letters, the opaque—I guess is a way to describe it—supervisory warning letters, and then, of course, the threats tied to the CAMELS rating as well.

What we know about any kind of currency, any kind of thing is, if it is a legitimate matter, which I would—or, a legitimate business, which this member certainly thinks that crypto is, then what is going to happen is, if there are simply attempts to stifle it. It is going to go somewhere else where it is allowed, whether it is in industries, I believe, banking with State-regulated banks or, many cases, going offshore.

Mr. Grewal, I will just ask this question to you. One, it does seem to me that, as U.S. regulators are impacting the American digital asset community, it would appear—and you can tell me if I am wrong—that it is impacting our ability to compete globally? If that is, in fact, the case, sir, are there any other countries that are more welcoming to that financial innovation?

Mr. GREWAL. Thank you, Congressman.

There is no question that the sclerosis that we have all operated under here in the United States for the last many years—I will put it that way—regarding legislation and regulation has led to a flight from the United States to other jurisdictions.

The Europeans, for example, have passed a market and crypto assets form of legislation that, while not perfect, offers a reliable, steady framework within which to operate. That has drawn capital; that has drawn jobs.

It was mentioned earlier, Singapore, is another global leader in cryptocurrency regulation. They, too, are drawing capital, jobs, and,

frankly, enthusiasm and creativity that belongs here in the United States.

While crypto is a global technology and a global industry, so much of the most important innovations actually were developed here in America. Yet, through this absence of regulation, this sclerosis, we have simply pushed entrepreneurs and risk-takers—appropriate risk-takers, the kind of risk-takers we used to be proud of in this country—to other parts of the world.

Mr. MOORE. Thank you very much.

Mr. Chairman, I yield back the balance of my time.

Chairman MEUSER. The gentleman yields.

The chair now recognizes Mr. Davidson of Ohio for 5 minutes.

Mr. DAVIDSON. Thank you, Chairman. Thanks for allowing me to waive on to this subcommittee. I am the Chairman for National Security and Illicit Finance. I have obviously been involved in digital assets and capital markets for a while but normally would not get to participate in this subcommittee, so thank you.

It is a great hearing topic. Under the last Congress, I was on the Weaponization Committee, and we dealt with Operation Choke Point, frankly. We looked at how banks were weaponizing the Bank Secrecy Act, really not of their own initiative but under pressure from regulators and, frankly, the Department of Justice and even the FBI, so thanks for coming.

Look, the idea that we are referring to this as “Choke Point 2.0” is pretty embarrassing because it means there was Choke Point 1.0., and that was under Obama, then under Biden, so we are noticing a theme. Hopefully we will be clear because Congress will take action to make sure that we lock in this electoral mandate to reject the weaponized government that we have seen and make the most of this market.

Just yesterday, having taken control of the FDIC from disastrous leadership, the Trump Administration released 175 documents.

Mr. Grewal, you highlighted a number of implications from some of those documents, but I just wanted to start with you and be clear that the targeting of the industry not only affected your company, but it affected Signature Bank. Barney Frank’s portrait is right up there, and he was on the board of Signature Bank. He said there was no solvency issue, the problem was they are banking crypto.

Did the improper seizure of Signature Bank scare the industry?

Mr. GREWAL. Yes, Congressman. The industry was not only scared, but they were also terrified. That was a bank that was meeting its customer requirements, fulfilling every regulatory obligation, and simply because it chose to put its business into the hands of the crypto industry and its customers it was effectively told to shut down.

Mr. DAVIDSON. Yes. They were targeted and, literally, the assets were seized.

Look, it kind of reminds me in a pasture, cows, not all of them have to hit the electric fence; They notice one of them hit the electric fence, and everybody else kind of get the memo, “Stay clear.” It seems like that was the intent.

Does anyone, kind of, disagree with that? Does that seem like that was the intent?

Mr. GREWAL. That was absolutely the intent.

Mr. DAVIDSON. Thank you.

You highlighted the collaboration that firms were doing with regulators. One of those, Mr. Campbell, in addition, as the—the FDIC would demand letters of inquiry. They would say, oh, give us a little more information, a little more information.

Did they ever reach a point where they had learned enough about the business model and say, “Oh, well, now we understand, you are green-lighted to go ahead and participate, you are safe and sound?” Did they ever do that?

Mr. CAMPBELL. No. As best we know, almost no bank was ever given approval for these actions.

Mr. DAVIDSON. I think there is a coordinating committee. I do not know really where they met or what the nexus was. Elizabeth Warren kind of wants to take credit for it. Gary Gensler met with her often. Lael Brainard from the FDIC, or the Federal Reserve System (Fed) kind of went into the administration and they seemed to be coordinated in the effort to shut down the industry.

I think that, if anything, you will see a coordinated approach to, kind of, deweaponize that and let the money be the money.

The reality is, we have seen for a long time—and, look, some of my colleagues highlighted it by saying, oh, it is targeting Black or Brown people or whatever. The reality is, unfortunately, at times in our country’s history, we have seen the financial services sector basically used as leverage to say, “Oh, well, you are not going to bank those people, are you?”

In this case, it really meant somebody with a business model. It did not mean that it was sound or unsound. It just meant, “We do not like you. You are not going to bank those kinds of people, are you?” That is exactly what the administration was doing to this entire sector.

Sadly, we are seeing that happen in other sectors. In nearly every State in the country, some form of marijuana is legal, but you see, kind of a second tier of backdoor making it illegal by saying, “Oh, well, you are not going to bank those people, are you?” People, whether they are investors, employees, or anything else, in a lawful sector are being debanked.

Ms. Olesiuk, could you give us some insight into what we could do about that?

Ms. OLESIUK. Thank you for the question, Congressman.

I think that we need to focus on, as I said earlier, the risk analysis of every—the regulators need to ensure that there is a proper risk analysis being done of the risk that is being taken on, and every lawful business, customer and person are entitled to access to the banking system.

Mr. DAVIDSON. Yes, we could pick up on that. We have done a lot. One of those bills was Secure and Fair Enforcement Regulation Banking Act (SAFER). Hopefully we will get something like that along the finish line as a result of this focus on Choke Point.

Thanks for the opportunity, and I yield back.

Chairman MEUSER. The gentleman yields.

Mr. Downing of Montana is now recognized for 5 minutes.

Mr. DOWNING. Thank you, Mr. Chairman.

Now, as Montana's former regulator for securities and insurance, my mission was to hold bad actors accountable, to lower insurance costs, and to reduce unnecessary regulations for Montana businesses. Tried to partner with business, tried to streamline that, while making sure that we do hold those bad actors accountable. My job was not to tell businesses who they can work with.

The priority of the regulators is safety and soundness. Under Joe Biden, the priority was picking winners and losers and pushing policies that could not get enacted through Congress, from suffocating fossil fuel companies to stifling digital asset innovation in the United States.

My first question: Mr. Grewal, can you tell me what you expect regulators to do to protect the safety and soundness of the digital asset ecosystem?

Mr. GREWAL. Thank you, Congressman.

I suppose, to put it as simply as I can, to say what they want us to do and, when we do it, to say what else we need to do in order to comply with their expectations.

It is the combination of refusing to lay out simple rules that we can all follow and, when they have questions with compliance with those rules, operating under the cloak of secrecy and using tactics such as delay and obfuscation to essentially exhaust the firm into submission.

Mr. DOWNING. Thank you.

Mr. Campbell, do regulators treat digital asset companies differently from other lines of business?

Mr. CAMPBELL. Yes, sir.

Mr. DOWNING. Yes.

Mr. Thiel, do you believe the Choke Point 2.0 scheme drives companies like yours out of the United States?

Mr. THIEL. Congressman, 2 years ago, we made the public statement that we were going to move 50 percent of our revenues offshore because of the regulatory environment we were operating in.

We grew at a very fast rate. We tripled our size in 2023. We doubled it again last year and will likely grow at a very large rate this year. We make investments, if you look at last year alone, of \$2 billion in the United States. That \$2 billion results in \$10 billion of gross domestic product (GDP) growth, jobs are created, people get schools paid for. In communities in Texas, our property taxes, alone, fund the fire department, the police department, and all sorts of public services.

The fact that we have to look to go offshore for that, which increases our cost of doing business, is the only way we can survive as a business when the regulatory environment is antagonistic to our business.

Mr. DOWNING. Thank you.

I am proud to represent Montana's Second District. It is very rural and sparsely populated.

Mr. Thiel, when companies are forced to shut down or exit due to unreasonable and political regulations, what is the future of innovation in States like Montana?

Mr. THIEL. Unfortunately, Congressman, innovation ceases to exist in those States when technology companies like ourselves move out of the State.

One of the downstream benefits for companies like us to come into States, especially rural States like Montana, is, we have to train technicians. We hire technicians; we up-skill them. We hire a lot of veterans, and we are a very proud employer of many veterans. We up-skill them so they are able to service these technology products that we put in the field, they are able to operate them, install them, manage them, monitor them and if we pull up stakes and go, there are not other jobs for them—

Mr. DOWNING. Right.

Mr. THIEL [continuing]. in those regions.

Mr. DOWNING. Thank you.

The United States must maintain its position as the hotbed for innovation around the world. Access to banking services is crucial for fostering growth and opportunity. If you take issue with an industry, you can always pass a law rather than allow unelected bureaucrats to foreclose on their ability to do business.

Thank you, Chairman, for holding this hearing. I am happy there is a new administration and Congress who value fostering innovation in the United States.

I yield back.

Chairman MEUSER. The gentleman yields.

The chair now recognizes the Ranking Member, Mr. Green, for 5 minutes, of Texas.

Mr. GREEN. Thank you, Mr. Chairman.

Permit me to ask, have any of you read some document from the Biden Administration or some regulator indicating that there is an Operation 2.0 Checkpoint—or Operation Choke Point 2.0? Have you—from the Biden Administration, that said “2.0”?

Okay, so this is a made-up statement. Somebody concluded that this is something that sells, so they have gone with “2.0.”

I was here in 2008 when we had the downturn, and it was never alleged that too much regulation caused the problem.

I was here when Bernie Madoff made off with more than \$60 billion. It was never alleged that too much regulation is what allowed him to do it.

Silvergate, Signature Bank—in fact, my colleagues have indicated that it was the regulators that caused the problem, a lack of regulation, not all, but some have.

The question becomes this: Do you want too much regulation, too little regulation, or do you want it to be the “Goldilocks,” just right? Would not we all?

The point is, given what is happening without guardrails as it relates to cryptocurrency—and I believe that—would you agree that we need some more guardrails? Anybody agree? Okay. If you agree, raise your hands. Just raise your hand, please.

Okay. Everybody agrees.

Where do the guardrails come from? Somebody might say Congress. Would you agree that Congress is the place where guardrails should emanate? Raise your hands, please.

Okay. Thank you.

For Congress to act, you have to have an act of Congress. Congress has not been able to act, for various and sundry reasons. I do not want to get into all of it, but the regulators are in a tough position.

I would not want to be a regulator. That is a tough job, because if a bank fails, then you did not do enough, and then if it somehow does not give you the kind of regulation that you want, it is too much. I would not want to be a regulator, but I do know this, I was here to receive all of the complaints in 2008 and all of the complaints in the 1960s. I think it was when Bernie Madoff performed his dastardly deed.

A good many people who want less regulation will not be here to receive the complaints. They come and they go, but there are some of us who have decided that we want to be here today and tomorrow and thereafter, and we have been fortunate enough and blessed enough to do it.

I am not going to get angry with regulators because those who are regulated contend that they are over-regulated. I want to fix a problem, but I am not going to take all of this and conclude that the regulators are over-regulating, when you all agree that there should be guardrails.

At some point, Congress has to act. I have seen Chairwoman Waters when she was chair and as ranking member. She and Mr. McHenry worked to try to give us the guardrails, but it is difficult to satisfy enough members to get something done.

If these banks fail, and you have a cascading event, we will find ourselves revisiting 2008. When Silvergate and Signature Bank, when they went under, one of our great fears was that this could become the start of a domino effect. I remember how hard our ranking member worked, with others, to try to prevent this.

I thank you for your testimony. I assure you, I am going to do what I can to make sure that you are being treated fairly, but if I am going to err, it would be on the side of regulating and not deregulating.

I yield back.

Chairman MEUSER. The gentleman yields.

The gentleman from Wisconsin, Mr. Steil, is now recognized for 5 minutes, the Chair of the Subcommittee on Digital Assets.

Mr. STEIL. Thank you very much, Mr. Chairman.

I appreciate all of you being here today. As Chairman of the Subcommittee on Digital Assets, I take great interest in this and appreciate you, Mr. Chairman, for waiving me on to the committee today on what has been an incredibly important conversation.

My colleague across the aisle, in his closing remarks for the minority, referenced that “Choke Point 2.0” might be a made-up statement, but I feel like that is as if you open the door of your home, the sidewalk and driveway is wet, and you conclude, “A-ha, but I did not see the rain.” It is pretty obvious what is going on when you actually look behind the hood and use common sense, just like if you opened your door and you look out and your driveway is wet, common sense tells you that it rained.

If we look at what played out in the Biden Administration through the regulators and what played out through their pause letters, which we have discussed today, through informal or offline means, it was pressure of financial institutions to debank digital asset firms and to make sure that those individuals understood that pressure was there across the ecosystem. I think that is what we really see today at today’s committee hearing.

It is the importance of not allowing—as we discovered in Choke Point 1.0 with our Second Amendment rights—not allowing the regulators to drive forward a political agenda through their authority as regulators to correctly assess risk across the system but not to put their finger on the scale as a result to their individual view of any given industry that the bank or financial system should be lending into.

I think that is kind of a stage-setting. What I want to do is dig in briefly, if I can. I will start with you, Mr. Campbell, and then I will move along.

I think one of the important parts here to discuss is, kind of, how bank examiners define traditional risk and how it is different from reputational risk. Succinctly, can you give me the difference between those because I want to build on that?

Mr. CAMPBELL. Yes. Reputational risk is essentially: we believe a bank is doing something that could damage its reputation in some ways that would cause customers to disfavor it, versus forms of business risk that are more objective, like you are lending to very risky people.

Mr. STEIL. Would reputational risk—could that be used as a shield for regulators to inject political objectives into the banking system?

Mr. CAMPBELL. It certainly could be, yes.

Mr. STEIL. Do you think that was the case as it relates to crypto investments?

Mr. CAMPBELL. There is a great example of that. Paxos ran Binance USD (BUSD) in New York. They have been regulating stablecoin since 2018 and thanks to regulatory pressure, that had to be shut down.

I have the privilege of having built one of two stablecoins that was above \$10 billion and went back to zero. We disrupted no markets, returned every penny. There was no danger to everybody and shutting it down benefited Tether.

Mr. STEIL. Let me jump to you, Mr. Grewal, if I can, to build on this. In your experience, how do regulators and banks think about reputational risk? To what extent does the political bias or policy bias of the regulators—how are they leveraging those two risks to drive their agenda?

Mr. GREWAL. Reputation in banking matters, Congressman. There is no question about it, but it is too often used as a catch-all or an excuse for other considerations that have no basis in law or, frankly, no basis in fairness.

There is no question that additional guidance from this Congress would be extraordinarily helpful in cabining or restricting the use of reputational risk to simply deem unacceptable all sorts of industries or individuals who happen to be out of political favor.

Mr. STEIL. I think, broadly speaking, as we wrap up today's hearing—and thank you, Mr. Chairman, for scheduling it—this is a broader point, that politics do not belong in our banking laws. What we want is the regulators, on their task, to analyze actual risk in the system rather than putting their finger on the scale to drive forward their own partisan, political, or social agenda.

Having today's hearing on Choke Point 2.0, in recognition that this really was occurring by the regulators inside the Biden Administration, I think is important.

I think it is a bit naive or attempting to discredit the facts to say that it is not occurring. Again, I go back to my analogy. If you open the door of your home and the pavement is wet and your driveway is wet, it rained. As we look back as to what happened inside our financial system under the Biden Administration, we could have a debate of whether or not you feel like you need more evidence, but I think the evidence is pretty clear, it rained. We need to stop this, and we have a real opportunity.

One final point. It was referenced that legislation did not get done in the previous Congress under the Biden Administration. The good news is, we have Republican-unified control, and I think we have a great opportunity for Congress to act. I look forward to working with everybody.

Mr. Chairman, I yield back.

Chairman MEUSER. The gentleman yields.

Before we adjourn, I am going to take a point of personal privilege and yield to the ranking member.

Mr. GREEN. Thank you again for your kindness, Mr. Chairman.

Mr. Chairman, sadly, today—and, to a certain extent, happily—we have one among us who is going on to bigger and better things. She has been an outstanding public servant, a brilliant, brilliant, brilliant asset to the committee, in that she has worked with us—many of the things that we have been able to do successfully we can attribute to her and her brilliance.

Today, Esther Kahng is going to be leaving us shortly. This is her last hearing, and I would hope that we respect her and appreciate her enough to give her a round of applause. [Applause.]

Mr. GREEN. With that, Mr. Chairman, I will yield back.

Chairman MEUSER. The gentleman yields.

We would certainly like to thank our witnesses for their testimony today.

I think it is clear we need the FDIC to provide clear guidance and regulatory responsibility for the digital asset industry. Congress and this committee will create a framework for digital assets regulation, but prudential regulators must immediately allow the crypto industry access to financial services.

Without objection, all members will have 5 legislative days within which to submit additional written questions for the witnesses to the chair.

Questions will be forwarded to the witnesses for their response. I ask our witnesses to please respond no later than March 31, 2025.

[The information referred to can be found in the appendix.]

Chairman MEUSER. This hearing is adjourned. Thank you all.

[Whereupon, at 3:48 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

2/5/25, 3:44 PM

Treasury Department Letter to Members of Congress Regarding Payment Systems | U.S. Department of the Treasury

An official website of the United States government [Here's how you know](#)

U.S. DEPARTMENT OF THE TREASURY

Treasury Department Letter to Members of Congress Regarding Payment Systems

February 4, 2025

I am writing in response to your letter ... regarding payment systems operated by the U.S. Department of the Treasury.

The Treasury Department's Bureau of the Fiscal Service (Fiscal Service) operates vital payment systems for the federal government, and those systems should promote financial integrity and operational efficiency. The Fiscal Service disburses nearly 90 percent of all federal payments, in over 1.2 billion transactions per year. Treasury is committed to ensuring that the Fiscal Service is functioning in a manner consistent with the highest levels of efficiency and in accordance with the expectations of taxpayers to prevent waste, fraud and abuse.

Treasury has no higher obligation than managing the government's finances on behalf of the American people, and its payments system is critical to that process. In keeping with that mission, Treasury is committed to safeguarding the integrity and security of the system, given the implications of any compromise or disruption to the U.S. economy. The Fiscal Service is confident those protections are robust and effective. Therefore, expanding on efforts that began under the prior Administration, Treasury has been undergoing a review of these systems to maximize payment integrity for agencies and the public.

Importantly, the ongoing review of Treasury's systems is not resulting in the suspension or rejection of any payment instructions submitted to Treasury by other federal agencies across the government. In particular, the review at the Fiscal Service has not caused payments for obligations such as Social Security and Medicare to be delayed or re-routed. To be clear, the agency responsible for making the payment always drives the payment process. Currently, Treasury staff members working with Tom Krause, a Treasury employee, will have read-only access to the coded data of the Fiscal Service's payment systems in order to continue this operational efficiency assessment. This is similar to the kind of access that Treasury provides to individuals reviewing Treasury systems, such as auditors, and that follows practices associated with protecting the integrity of the systems and business processes.

Mr. Krause is conducting this effort in coordination with veteran career Treasury officials, and all operational processes continue to be conducted only by career Treasury staff in accordance with all standard security, safety, and privacy standards. Mr. Krause is a longtime technology executive. His decades of experience in building companies and managing balance sheets as a chief financial officer are of great benefit to this review. In order to allow him to perform this function, he has been hired as an expert/consultant by the federal government and designated in a role commonly used across Administrations—a "special government employee"—pursuant to applicable law. This role involves a hiring process that includes a review of a candidate's credentials and background, and demands the same ethical standards of privacy, confidentiality, conflicts of interest assessment, and professionalism of other government employees.^[1] These assessments are conducted by career legal and ethics officials. Mr. Krause is subject to the same security obligations and ethical requirements, including a Top Secret security clearance.

Treasury will continue its efforts to promote efficiency and effectiveness in its operations, and to prevent waste, fraud, and abuse.

[1] See

<https://extapps2.oge.gov/Training/OGETraining.nsf/xsp/.ibmmmodres/doino/OpenAttachment/training/ogetraining.nsf/D006291C1FEC02448525869>



215 Pennsylvania Avenue, SE • Washington, D.C. 20003 • 202/546-4996 • www.citizen.org

February 6, 2025

The Honorable French Hill, Chair
The Honorable Maxine Waters, Ranking Member
Honorable Members
House Financial Services Committee
Washington, DC 20515

Dear Committee members,

On behalf of more than 500,000 members and supporters of Public Citizen¹, we attach a letter sent to federal officials regarding President Trump's recent cryptocurrency foray. The House Financial Services Committee scheduled two hearings on crypto currency: on February 6, 2025, the Committee titles a hearing, "The Biden Administration's Effort to Put Crypto in the Crosshairs;" and on February 11, 2025, a hearing titled "A Golden Age of Digital Assets." We urge members to explore the Trump meme during these hearings.

The Trump meme crypto effort hardly represents a "golden age" but rather something that should be put in the "crosshairs." This meme, as the President says, is merely "an idea" meant to celebrate his leadership. By his own account, it is not an investment. Those who send Trump money receive a digital receipt (on a blockchain) that is no different than a digital bank record of a payment received. As the attached letter describes, even crypto sympathizers deride such meme coins.

For questions, please contact Bartlett Naylor at bnaylor@citizen.org.

Sincerely,

Public Citizen

¹ Public Citizen is a nonprofit consumer advocacy organization with members in all fifty states. Public Citizen regularly appears before Congress, administrative agencies, and courts to support the enactment and enforcement of laws protecting consumers, workers, and the general public.



215 Pennsylvania Avenue, SE • Washington, D.C. 20003 • 202/546-4996 • www.citizen.org

February 5, 2025

John Keller, Chief
Public Integrity Section
Department of Justice
950 Pennsylvania Ave
Washington, D.C. NW
20530-0001

David Huitema, Director
U.S. Office of Government Ethics
250 E Street, SW., Suite 750
Washington, DC 20024

Dear Officers,

We ask you to investigate whether President Donald J. Trump has violated 18 U.S.C. § 201, as implemented in 5 C.F.R. § 2635, barring the president from soliciting gifts.

Federal law strictly regulates payments to government officials, including gifts. Although the president may receive gifts, he may not "[solicit](#)" gifts. These prohibitions begin with the Constitution's Emoluments Clause and are reiterated in the anti-bribery statute, 18 U.S.C. § 201, and federal regulations, 5 C.F.R. § 2635. Although [section 2635.205](#) lists several exemptions from the prohibition, none exempts soliciting purchases for personal gain.

As the [Congressional Research Service](#) has explained:

Under these regulations, the President is expressly exempt from the broad restrictions on receiving or accepting gifts from prohibited sources or gifts given because of his official position, and thus may accept gifts from the general public, even from "prohibited sources," or gifts given because of his official position, as long as the President does not "[solicit](#) or coerce" the offering of gifts from such sources, nor accept a gift in return for an official act. [Emphasis added.]

President Trump's promotion of a Trump meme appears to violate this prohibition. In a January 17 tweet, also apparently retweeted after January 20, [Trump stated](#): "My NEW Official Trump Meme is HERE! It's time to celebrate everything we stand for: WINNING! Join my very special Trump Community. GET YOUR \$TRUMP NOW. Go to <http://gettrumpmemes.com> — Have Fun!" On Truth Social, [he posted the same content](#), on January 21, at 6:19 PM.

Trump is the principal owner of the Trump Meme. The [website](#) explains that the memes are largely (80 percent) owned by CIC Digital LLC, "an affiliate of The Trump Organization." CIC Digital is [100% owned](#) by the Donald J Trump Revocable Trust. Donald Trump is the "[sole beneficiary](#)" of the revocable trust. Under the question [on the website](#): "Is this an official Trump product?" the website answers: "Yes, this is the only Official Trump Meme, by President Donald J. Trump."

As to why the public might be interested in sending money, the [website explains](#): "On July 13, 2024, President Trump faced death and came up fighting! With his fist in the air and the iconic battle cry FIGHT FIGHT FIGHT, President Trump showed the world what a LEADER is made of. His strength and courage ignited a movement becoming the most memorable meme of the century. Now, you can get your piece of history. This Trump Meme celebrates a leader who doesn't back down, no matter the odds. Join the Trump Community - we're all about fighting for what matters. "Under [the Trump meme website's question](#), "What is a meme?" the website explains: "Merriam-Webster's meme noun: 1: an idea, behavior, style, or usage that spreads from person to person within a culture."

The [website states](#) that "Trump Memes . . . are not intended to be, or to be the subject of, an investment opportunity, investment contract, or security of any type."

Accordingly, a person sending money for a Trump meme is not purchasing a tangible product. Instead, the person receives only a digital receipt (in a blockchain), which is similar to a donor sending a check and receiving digital confirmation that the check was received.

Beyond Trump's own declaration that the Trump meme is not an investment, other cryptocurrency observers deride memes generally as without value. [Former aide Anthony Scaramucci](#) said Trump's effort demeans broader cryptocurrency efforts, calling it "Idi Amin level corruption." Another [commenter](#) said that the Trump meme "is effectively a 'for sale' sign on the White House." Some, including an author in the Washington Post, characterized this token as a "[sh—coin](#)."

In short, it appears Trump is not soliciting money in exchange for an investment or tangible product (such as a [Bible, sports shoes, or a guitar](#)), but soliciting money in exchange for nothing—that is, asking for a gift that will benefit him personally.

Beyond the issue of solicitation, the Constitution (Article 1, Section 9) forbids accepting money (specifically a "present" or "emolument") or anything of value from any "king, prince, or foreign state." Because of the nature of a cryptocurrency exchange, it is difficult to know whether foreign state actors are gifting the president by way of purchasing a Trump meme. We urge you to investigate this issue, as well.

The dangers inherent in the Trump meme portend ominously. Should the president be allowed to enrich himself in this way, other politician might follow this path, rendering the prohibition on solicitation in 18 U.S.C. § 201 and the prohibitions on receipt of gifts by officials other than the president virtually meaningless.

Therefore, we ask the Office of Government Ethics and the Department of Justice to investigate this arrangement to determine whether it constitutes an impermissible gift solicitation. If the DOJ and OGE find in the affirmative, we ask that they make appropriate recommendations, including termination of the meme sale, return of monies, and any other available remedies.

For questions, please contact Bartlett Naylor at bnaylor@citizen.org; and/or Dr. Craig Holman at cholman@citizen.org,

Sincerely

Bartlett Naylor
Public Citizen

Dr. Craig Holman
Public Citizen

January 31, 2025

The Honorable Dan Meuser
Chairman

The Al Green
Ranking Member

House Financial Services Subcommittee on Oversight and Investigations
Washington, DC 20510

Dear Chairman Meuser and Ranking Member Green:

We strongly support your willingness to investigate the issue of debanking under Operation Chokepoint 2.0, but as one of the most frequent targets of debanking, the state-legal cannabis industry cannot be left out of policy solutions that look to resolve the issue of debanking. The state-legal cannabis industry operates in 39 states and employs over 440,000 workers nationwide, generating over \$32 billion dollars in revenue in 2024.¹² However, due to discrepancies between state and federal laws in the United States, the cannabis industry and its employees have been frequently targeted by regulators and financial institutions alike.

State-legal and approved cannabis businesses are routinely debanked and excluded from financial services that would increase public safety and financial transparency. So too are the businesses' employees — from executives down to part-time workers who are denied home loans, mortgages, and even have family members' accounts frozen because of perceived involvement with the cannabis industry.³ Even more objectionable, organizations that simply exercise their First Amendment rights of advocating for *changes* in the laws related to cannabis have been debanked, even when these organizations do not actually touch or process cannabis themselves.⁴ State governments who have authorized cannabis sales have also faced challenges in maintaining financial services.⁵

A lack of access to financial services for the cannabis industry has created numerous problems that are all too familiar for those who have been debanked, including but not limited to:

Account Closures: Many cannabis related businesses have had their business accounts closed, despite operating in compliance with state laws, and having approval from state unable to conduct even the most basic of business operations

Personal Banking Issues: Individual employees have been unable to secure mortgages, auto loans, or other personal loans because of their association with cannabis, creating significant impacts on financial stability and life planning

Higher Operational Risks: A lack of access to traditional financial services leads to cannabis businesses operating primarily in cash. A high volume of cash creates security

¹ <https://www.newsweek.com/us-marijuana-industry-all-time-high-jobs-sales-1891143>

² <https://businessofcannabis.com/us-cannabis-sales-to-hit-32bn-this-year-as-industry-continues-record-growth/>

³ <https://www.businessinsider.com/cannabis-executives-and-employees-cant-get-mortgages-accounts-2022-6>

⁴ <https://www.cincinnati.com/story/news/2017/07/13/card-denied-marijuana-advocacy-groups-bank-account-terminated/471637001/>

⁵ <https://cnsmaryland.org/2023/04/05/federal-banking-rules-make-funding-maryland-cannabis-industry-tricky/>

concerns for communities and businesses alike and has led to a string of violent robberies at dispensaries nationwide.⁶ Due to ongoing conflict between federal and state law, many insurance providers are also unwilling to work with cannabis businesses.⁷

Difficulty in Tax Collection: The debanking of cannabis businesses complicates how tax payments are collected. Businesses must physically deliver tax payments to collection offices, creating a burden both on the business and the tax collector.

Limited Growth Opportunities: Even when banking services are offered they are limited—while some banks and credit unions are willing to work with the cannabis industry, it results in costly monthly fees, and limited access to loans, credit lines, and electronic payment processing. Additionally, cannabis companies are barred from listing on the United States capital markets.

There is a turnkey legislative solution that ends Operation Chokepoint and ensures that state legal cannabis businesses don't face the issue of debanking. Initiatives like the SAFE Banking Act would create a financial safe harbor for cannabis businesses and employees but would also end Operation Chokepoint by requiring regulators to have actual valid reasons for account termination rather than perceived risk. The SAFE Banking Act does **not** federally legalize cannabis; it does **not** change criminal penalties associated with conduct related to cannabis; and it does **not** require banks to service cannabis businesses. The SAFE Banking act merely **allows** financial institutions to serve state legal and licensed businesses and those interacting with the state-legal industry without fear of retribution.

No business should be at risk of being debanked, especially if it complies with state licensing and regulation requirements. We appreciate your consideration and look forward to the development of a policy solution that ends Operation Chokepoint and ceases debanking within the state legal cannabis industry.

Sincerely,

The United States Cannabis Roundtable

CC: Members of the Subcommittee on Oversight and Investigations



The United States Cannabis Roundtable (USCR) was formed in 2025, combining the National Cannabis Roundtable and the United States Cannabis Council. The organization represents all facets of the state-legal cannabis industry from large multistate operators down to individual license holders, service providers, and ancillary businesses.

⁶<https://abc3340.com/news/local/cannabis-cash-rise-in-robberies-as-banks-wont-take-money-from-medical-marijuana-businesses-alabama-gadsden-crime/>

⁷https://www.ct.gov/ins/related/20220329_Connecticut%20Insurance%20Department%20Reports/2022%20Cannabis%20Insurance%20Report.pdf



Jason Stverak
Chief Advocacy Officer

1627 Eye St. NW
Suite 935
Washington, DC 20006
202.734.5007
www.d cuc.org

February 3, 2025

The Honorable Dan Meuser
Chairman
Oversight and Investigations Subcommittee
Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

The Honorable Al Green
Ranking Member
Oversight and Investigations Subcommittee
Financial Service Committee
United States House of Representatives
Washington, DC 20515

Dear Chairman Meuser and Ranking Member Green:

On behalf of the Defense Credit Union Council (DCUC), I am writing to express our concerns regarding the growing issue of debanking and to highlight the pivotal role that credit unions play in safeguarding access to essential financial services for all Americans. As the Committee prepares for the upcoming hearing entitled "[Operation Choke Point 2.0: The Biden Administration's Efforts to Put Crypto in the Crosshairs](#)," we believe it is crucial to recognize how credit unions serve as a vital counterbalance to discriminatory and unjust financial exclusion.

DCUC represents credit unions stateside and overseas serving military and veteran communities as well as their families, encompassing over 40 million members and having over \$525 billion in assets. We believe it is crucial to address specific issues pertinent to our members during this confirmation process.

Debanking, the practice of financial institutions terminating or restricting services to certain businesses or individuals without clear justification threatens financial inclusion and economic stability. This issue disproportionately affects small businesses, entrepreneurs, and underserved communities, including military families and veterans who rely on access to fair and stable financial services. Debanking can occur due to opaque risk assessments, subjective compliance concerns, or the consolidation of financial services into fewer, larger institutions that prioritize profit over people.

Unlike large for-profit banks, credit unions are member-owned, community-focused institutions that prioritize financial inclusion. Because credit unions operate under a cooperative model, they are not driven by quarterly profit margins but by the needs of their members. This structure makes credit unions a critical safeguard against debanking and financial discrimination.

Credit Unions Protect Against Debanking in Several Key Ways:

A Mission of Inclusion: Credit unions were founded on the principle of financial cooperation, ensuring that underserved and marginalized groups including low-income families, veterans, and small business owners are not left without banking options. Credit unions do not engage in arbitrary service terminations based on corporate risk calculations; instead, they assess the needs of their members and provide personalized financial solutions.

Serving Those Who Serve Our Country

Community-Centric Decision-Making: Credit unions are deeply embedded in the communities they serve, understanding the local economy and unique financial needs of their members. This prevents the kind of impersonal, automated decision-making that often leads to unjust debanking.

Commitment to Fair and Transparent Practices: Many instances of debanking arise from vague or unexplained risk concerns tied to regulatory compliance. Credit unions are subject to stringent oversight while remaining transparent and accountable to their members, ensuring that account closures or restrictions are based on clear, legitimate concerns rather than arbitrary de-risking strategies.

Veteran and Military Support: As an organization dedicated to serving defense credit unions and military communities, DCUC understands how debanking disproportionately impacts service members, veterans, and their families. Many commercial financial institutions have withdrawn from military bases or imposed excessive fees on accounts, leaving our nation's heroes without accessible financial services. Credit unions step in where big banks pull out, ensuring that military families have access to affordable banking and lending products.

Small Business and Entrepreneurial Support: Many small businesses, particularly those in politically disfavored industries or new startups without an extensive financial history, face debanking at an alarming rate. Credit unions serve as lifelines for these businesses, providing fair access to capital and financial services that would otherwise be denied by large banks focused on reducing risk exposure rather than supporting local economies.

The recent article published by CU Today, [Credit Unions: A Reliable Shield Against the Growing Crisis Of Debanking](#), underscores the essential role that credit unions play in mitigating this crisis. By prioritizing relationships over risk modeling, credit unions offer a financial safety net to individuals and businesses unfairly targeted by debanking practices. ([cutoday.info](#))

As the Committee examines the real impacts of debanking in America, we urge you to support policies that empower credit unions to continue providing fair and equitable financial services. This includes ensuring that regulatory policies do not inadvertently force credit unions into the same de-risking behaviors as large banks and that financial inclusion remains a top priority in financial oversight discussions.

Thank you for your attention to this critical issue. DCUC and our member institutions stand ready to work with the Committee to ensure that all Americans especially those who have served our country have access to stable, transparent, and inclusive financial services.

Should you or your team have any questions or desire additional information, please do not hesitate to contact me at 202.557.8528 or by email at jstverak@dcuc.org.

Sincerely,



Jason Stverak
Chief Advocacy Officer
DCUC

CC: HFSC Committee Members

FRENCH HILL, AR
CHAIRMAN



MAXINE WATERS, CA
RANKING MEMBER

United States House of Representatives
One Hundred Nineteenth Congress
Committee on Financial Services
2124 Rayburn House Office Building
Washington, DC 20515

Questions for the Record
Sub-Committee on Oversight and Investigations, entitled "Operation Choke Point 2.0: The Biden Administration's Efforts to Put Crypto in the Crosshairs"
February 06, 2025

Ranking Member Maxine Waters:

Mr. Paul Grewal

Which of the following options best describes your self-identified race? (you may choose more than one)

- a. White or Caucasian
 - b. Black or African American
 - c. Hispanic/Latinx
 - d. Asian
 - e. Middle Eastern/North African
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)
2. Which of the following options best describes your gender identity?
- a. Woman
 - b. Man
 - c. Non-binary
 - d. Transgender Man
 - e. Transgender Woman
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)

FRENCH HILL, AR
CHAIRMAN



MAXINE WATERS, CA
RANKING MEMBER

United States House of Representatives
One Hundred Nineteenth Congress
Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Questions for the Record
Sub-Committee on Oversight and Investigations, entitled “Operation Choke Point 2.0: The Biden Administration’s Efforts to Put Crypto in the Crosshairs”
February 06, 2025

Ranking Member Maxine Waters:

Mr. Fred Thiel

1. Which of the following options best describes your self-identified race? (you may choose more than one)
 - a. White or Caucasian
 - b. Black or African American
 - c. Hispanic/Latinx
 - d. Asian
 - e. Middle Eastern/North African
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)
2. Which of the following options best describes your gender identity?
 - a. Woman
 - b. Man
 - c. Non-binary
 - d. Transgender Man
 - e. Transgender Woman
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)

FRENCH HILL, AR
CHAIRMAN



MAXINE WATERS, CA
RANKING MEMBER

United States House of Representatives
One Hundred Nineteenth Congress
Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Questions for the Record

Sub-Committee on Oversight and Investigations, entitled "Operation Choke Point 2.0: The Biden Administration's Efforts to Put Crypto in the Crosshairs"
February 06, 2025

Ranking Member Maxine Waters:

Ms. Shayna Olesiuk

1. Which of the following options best describes your self-identified race? (you may choose more than one)
 - a. White or Caucasian
 - b. Black or African American
 - c. Hispanic/Latinx
 - d. Asian
 - e. Middle Eastern/North African
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)
2. Which of the following options best describes your gender identity?
 - a. Woman
 - b. Man
 - c. Non-binary
 - d. Transgender Man
 - e. Transgender Woman
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)