Cooper & Kirk
Lawyers
A Professional Limited Liability Company
1523 New Hampshire Avenue, NW
Washington, DC 20036

Operation Choke Point 2.0:
The Federal Bank Regulators Come For Crypto

David H. Thompson
John D. Ohlendorf
Harold S. Reeves
Joseph O. Masterman

TABLE OF CONTENTS

Page

I. Executive Summary 1

II. History Repeats Itself: The Rise of Operation Choke Point 2.0. 3

A. Operation Choke Point 1.0. 3

B. Operation Choke Point 2.0 and the Prudential Bank Regulators' War on the Innovation of the Blockchain. 7

1. The Prudential Bank Regulators Issue Informal Guidance Warning Banks of the Risks of Serving Crypto Businesses. 7

2. The Banks Feel the Pressure to Refuse to Accept New Crypto Customers and to Drop Crypto Customers. 11

3. Shuttering banks that serve crypto. 14

4. The Federal Bank Regulators Refuse to Charter Banks that Serve the Crypto Industry. 20

III. The Agencies' Backroom War Against Crypto is Unlawful and Unconstitutional, As Well As Arbitrary, and Capricious. 23

A. Operation Choke Point 2.0 is Unconstitutional. 23

1. Operation Choke Point 2.0 Violates the Due Process Clause. 23

2. Operation Choke Point 2.0 May Violate Structural Constitutional Protections. 27

B. The Federal Bank Regulators Are Failing To Perform Their Statutory Duties. 27

1. The Bank Regulators are Exceeding their Statutory Authority. 27

2. The Federal Banking Regulators are Not Performing their Statutory Duties. 28

C. The Prudential Bank Regulators are Violating the Administrative Procedure Act. 29

1. The Prudential Bank Regulators Have Acted Beyond Their Statutory Authority. 29

2. The federal bank regulators have evaded the notice and comment rulemaking requirements of the Administrative Procedure Act. 30

3. The Agencies have acted arbitrarily and capriciously by denying access to the banking system to new technologies they do not understand. 32

IV. Congress Should Perform its Duty and Rein in these Regulatory abuses. 33

I. Executive Summary

Recent stories in the financial press have uncovered a coordinated campaign by prudential bank regulators to drive crypto businesses out of the financial system. Bank regulators have published informal guidance documents that single out cryptocurrency and cryptocurrency customers as a risk to the banking system. Businesses in the cryptocurrency marketplace are losing their bank accounts, or their access to the ACH network, suddenly, and with no explanation from their bankers. The owners and employees of cryptocurrency firms are even having their personal accounts closed without explanation. And over the past two weeks, federal regulators have shut down a solvent bank that was known to be serving the crypto industry and, although it is required to resolve banks through the "least cost resolution" to the Deposit Insurance Fund, the FDIC chose to shutter rather than sell the part of the bank that serves digital asset customers, costing the Fund billions of dollars.

This pattern of events is not random, and we have seen it before. This is not the first time that federal bank regulators, working with their State-level counterparts, have abused their supervisory authority to label businesses unworthy of having a bank account and worked in secret to purge disfavored lines of commerce from the financial system. Beginning in 2012, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Board of Governors of the Federal Reserve System carried out a coordinated campaign to weaponize the banks against industries that had fallen out of favor with the administration—including gun stores, pawn shops, tobacco stores, payday lenders, and a host of other brick and mortar businesses. That campaign was called Operation Choke Point.

Our firm successfully challenged Operation Choke Point, and it was brought to a halt. The current bout of **regulatory overreach against the crypto industry is illegal** for much the same as reason as its predecessor. Specifically:

- Operation Choke Point 2.0 deprives business of their constitutional rights to due process in violation of the Fifth Amendment. It is well settled that when a federal agency attaches a derogatory label to an individual or business, and this stigmatizing label causes the business to lose a bank account or broadly precludes them from the pursuit of their chosen trade, the agency has violated the Due Process Clause of the Fifth Amendment, unless if first afforded the individual or business a right to be heard. This is precisely what the federal bank regulators responsible for Operation Choke Point 2.0 have done and continue to do by labeling crypto businesses a threat to the financial system, a source of fraud and misinformation, and a risk to bank liquidity.

- Operation Choke Point 2.0 violates both the non-delegation doctrine and the anticommandeering doctrine, depriving Americans of key structural constitutional protections against the arbitrary exercise of governmental power.

- By leveraging their authority over the banks to acquire the power to pick and choose the customers whom the banks may serve, the bank regulators have exceeded their

statutory authority. The bank regulators are charged with supervising the safety and soundness of the banks; their effort to anoint themselves the gatekeepers of the financial system and the ultimate arbiters of American innovation and American economic life cannot be permitted to stand.

- The federal bank regulators are also refusing to perform their non-discretionary duties when doing so will benefit the cryptocurrency industry. State banks that are statutorily entitled to access the federal reserve system are being denied their rights solely because they serve the crypto industry. The federal bank regulators are not free to pick and choose which statutory obligations they duties they wish to perform.

- The federal bank regulators are evading the notice and comment rulemaking requirements of the administrative procedure act by imposing binding requirements on the banking industry through informal guidance documents. This is undemocratic, since it deprives the public of the right to comment on proposed rules, and it also runs contrary to the principle of judicial review, since courts lack the power to review "informal" agency actions.

- Finally, the federal bank regulators are acting in an arbitrary and capricious fashion by failing to adequately explain their decisions, by failing to engage in reasoned decisionmaking, and by failing to treat like cases alike. It is difficult to imagine a more arbitrary and capricious agency action than simultaneously placing a solvent bank into receivership solely because it provided financial services to the crypto industry, while permitting insolvent institutions not tied to the crypto industry to continue operating.

We therefore urge Congress to perform its oversight role and hold these agencies to account. In section IV of this paper, we propose a series of questions that need to be answered—and a series steps that Congress should take in an effort to obtain those answers.

- ***First***, Congress should require the bank regulators to produce their communications with supervised financial institutions and state regulatory agencies regarding the denial or regulation of access to the financial system by crypto businesses and banks that serve the crypto industry.

- ***Second***, Congress should require the federal bank regulatory agencies to explain the basis for their conclusion that the safety and soundness of the financial system require the insulation of the banks from blockchain technology, from customers who operate in the crypto space, and from state-chartered depository institutions that are currently serving those customers.

- ***Third***, Congress should make clear to the federal bank regulators, and all federal agencies, that the notice and comment rulemaking requirements of the

Administrative Procedure Act are not optional. The requirements imposed by the APA are not obstacles to be evaded by the use of informal guidance documents.

- ***Fourth***, Congress should investigate the role of federal regulators in the decision by the New York Department of Financial Supervision's decision to shutter Signature Bank. Congress should also determine the FDIC's role in excluding bidders who wished to acquire Signature's digital asset businesses from the bidding process.

- ***Fifth***, Congress should investigate whether bank regulators are acting to squelch private sector innovation in order to clear the field of competition for the benefit of existing federally regulated banks or for a federal cryptocurrency alternative.

The persistent unwillingness of the nation's bank regulators to follow the law and obey the Constitution calls out for Congressional action. Cracks are starting to form in the American financial system as its regulators increasingly abuse their power to achieve aims outside their authority and beyond their competence.

II. History Repeats Itself: The Rise of Operation Choke Point 2.0.

A. Operation Choke Point 1.0.

Beginning in 2012, the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), and the Board of Governors of the Federal Reserve System ("the Federal Reserve"), with the prompting and the assistance of the Obama Administration's Department of Justice, conspired to choke off and strangle disfavored lines of commerce by depriving them of their access to the financial system. Reputations were tarnished through a whisper campaign carried out by federal bank examiners. Law-abiding businesses that presented no threat to the safety and soundness of the banking system had their ability to open a bank account or even to deposit a check now taken from them. Runaway regulators, acting well beyond their statutory authority and without any regard for the rule of law, deprived American businesses of their good names, of their right to pursue their chosen line of trade, and of their very right to exist, without affording them any right to defend themselves or to respond to the charges secretly being leveled against them. This campaign was dubbed Operation Choke Point by the federal regulators themselves, since it worked by "choking off" the disfavored business from access to the modern financial system.

Operation Choke Point had two components: the publication of informal guidance documents by the prudential bank regulators and a covert campaign of coercion, threats, and backroom pressure carried out by agency examiners and officials. The federal bank regulators first published a series of guidance documents, policy statements, and informal articles advising the financial institutions that they supervised to structure their account agreements with a selection

of "risky" customers to "permit immediate account closure [and] contract termination."[1] They also warned the banks to be wary of customers who maintained banking relationships with more than one bank, a practice that the businesses in the regulators' crosshairs would, predictably, soon be forced to adopt in order simply to survive.[2] These informal guidance documents paved the way for the campaign of regulatory coercion that was to come.

The critical fulcrum of Operation Choke Point, however, was the redefined concept of "reputation risk" that was promulgated through these informal guidance documents. A series of guidance documents redefined the concept of "reputation risk" in a manner that was vague, manipulable, and wholly foreign to customary bank examination practices. Slowly and incrementally, the prudential bank regulators transformed reputation risk from a requirement that a bank take care to guard its own good name,[3] which could be damaged when the services provided by the bank and its agents failed to measure up to customer expectations, to a concept that required banks first to evaluate the reputations of third parties with whom the bank does business, even when that third-party provides no customer-facing services on behalf of the bank, and finally to evaluate the reputations of the bank's customers.

---

[1] FDIC, Financial Institution Letter: Revised Guidance on Payment Processor Relationships, FIL-3-2012 (Jan. 31, 2012), available at https://www.fdic.gov/news/financial-institution-letters/2012/fil12003.html

[2] FDIC, Managing Risks in Third-Party Payment Processor Relationships, SUPERVISORY INSIGHTS, Summer 2011, at 3.

[3] As traditionally understood in the banking industry and as previously defined by the agencies, "reputation risk" reflects "the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions." FRB, Supervisory Letter: Risk-focused Safety and Soundness Examinations and Inspections. SR 96-14 (May 24, 1996), available at https://www.federalreserve.gov/boarddocs/SRLETTERS/1996/sr9614.htm. See also OCC, Risk Management Guidance: Third Party Relationships, OCC Bull. No. 2001-47 (Nov. 1, 2001) ("Reputation risk is the risk to earnings or capital arising from negative public opinion."), available at https://www.occ.gov/static/rescinded-bulletins/bulletin-2001-47.pdf; FDIC, Foreign-Based Third-Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships, FIL-52-2006 (June 21, 2006) ("Reputational risk is the risk that potential negative publicity about a financial institution's business practices will cause a decline in the customer base, costly litigation, or the loss of revenue."), available at https://www.fdic.gov/news/financial-institution-letters/2006/fil-52-2006.pdf. As previously defined by these three agencies, therefore, reputation risk was exclusively the risk that a bank might suffer harm to its reputation either by itself failing to serve its customers well or by contracting with a third party provider who then, acting in the bank's name, failed to serve those customers well. See, e.g., OCC, Risk Management Guidance: Third Party Relationships, OCC Bull. No. 2001-47 (Nov. 1, 2001), available at https://www.occ.gov/static/rescinded-bulletins/bulletin-2001-47.pdf; FDIC, Foreign-Based Third-Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships, FIL-52-2006 (June 21, 2006), available at https://www.fdic.gov/news/financial-institution-letters/2006/fil-52-2006.pdf.

The threat created by requiring banks to stand in judgment of their customers was recognized and understood even at the time. As Congressman Hensarling warned early in 2014, this newly-defined concept of reputation risk could easily "be invoked to compel a depository institution to sever a customer relationship with a small business operating in accordance with all applicable laws and regulations but whose industry is deemed 'reputationally risky' for no other reason than that it has been the subject of unflattering press coverage, or that certain Executive Branch agencies disapprove of its business model."[4]

And the banks were most certainly not left to decide for themselves when an individual customer's reputation required their banishment from the financial system. The prudential bank regulators made clear that only specific industries—those that were out of favor with the administration or with the federal regulators themselves—presented reputational risks to the banks that served them. In the summer of 2011, FDIC warned the banks of the heightened reputational risks associated with doing business with specific groups of merchants.[5] FDIC identified 30 merchant categories, including gun dealers, ammunition sellers, pawn shops, and payday lenders that were engaged in what the agency had deemed to be reputationally risky activities. And, of course, pornography, online gambling, and even racist materials were included on the list to create that "good picture regarding the unsavory nature of the businesses at issue" that the bank regulators were striving to create.

Indeed, bank regulators went to extraordinary lengths to smear the disfavored businesses. For example, FDIC personnel ensured that Chairman Gruenberg's talking points and correspondence with Congress always mentioned pornography alongside payday lending in an effort to convey a "good picture regarding the unsavory nature of the businesses at issue."[6] One official candidly explained that "including payday lenders in the same circle as pornographers and on-line gambling businesses will ultimately help with the messaging on this issue."[7]

---

[4] Letter from Rep. Jeb Hensarling, Chairman, H. Comm. on Fin. Servs., to Janet Yellen, Chair, The Fed. Reserve Sys. (May 22, 2014).

[5] FDIC, Managing Risks in Third-Party Payment Processor Relationships, SUPERVISORY INSIGHTS, Summer 2011, at 3.

[6] STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 113TH CONG., FEDERAL DEPOSIT INSURANCE CORPORATION'S INVOLVEMENT IN "OPERATION CHOKE POINT," at 10 (Dec. 8, 2014) [hereinafter "REP."], *quoting* email from a Counsel, Legal Division, FDIC, to Marguerite Sagatelian, Senior Counsel, Consumer Enforcement Unit, FDIC (Aug. 28, 2013 9:32), FDICHOGR00007424, available at https://oversight.house.gov/wp-content/uploads/2014/12/Staff-Report-FDIC-and-Operation-Choke-Point-12-8-2014.pdf

[7] Rep. at 11, *quoting* email from a Counsel, Legal Division, FDIC, to Marguerite Sagatelian, Senior Counsel, Consumer Enforcement Unit, FDIC (Aug. 28, 2013 9:32), FDICHOGR00007424. Pornography was among the first targets of Operation Choke Point. Citing "compliance issues," banks began in early 2013 to close the accounts not only of adult entertainment businesses, but also of hundreds of individual actors and actresses in the industry. J.P. Morgan Chase closed the accounts of former porn actress Teagan Presley and her husband, who had never been part of the business. The bank also refused to renew the home mortgage of studio head Marc Greenberg on account of "reputational risk." See Mary Emily O'Hara, *Is the*

Of course, Operation Choke Point had nothing to do with reputation or reputational risk, much less with bank safety and soundness. Instead, the personal biases of the banking regulators determined which businesses would be targeted for financial exile. Evidence soon emerged that payday lenders were being targeted because agency officials found them "unsavory,"[8] and believed payday lending was "a particularly ugly practice."[9] One senior official even admitted that he "literally [could] not stand pay day lending" and that he "sincerely" and "passionate[ly]" believe[d] that payday lenders "do not deserve to be in any way associated with banking."[10]

Having laid the groundwork by labeling these lawful businesses reputationally risky, the federal bank regulators, working together with their state counterparts, turned to the task of purging their accounts from each of the banks subject to their supervision. In the back rooms of banks around the country, bank examiners explained that those financial institutions that continued to serve customers that the federal regulators had labeled "reputationally risky" would suffer the consequences. As one examiner reportedly told a banker who hesitated to succumb to this pressure: "I don't like this product and I don't believe it has any place in our financial system . . . Your decision to move forward will result in an immediate, unplanned, audit of your entire bank." The message could not be clearer: "Turn against your customers, or your regulators will turn against you."

In the end, no bank that wants to remain in business can stand up to their prudential regulator forever. For over two years, the nation's gun dealers, pawn shops, tobacco stores, and payday lenders watched as one bank after another yielded to this campaign of regulatory coercion and closed their accounts. In the vast majority of these cases, no explanation was ever provided by the banks. This is unsurprising; it is the rare bank that will bear witness against its prudential regulator. These businesses thus had no opportunity to defend their good names from the regulatory smear campaign. They had no way even of knowing that it was their own government that was trying to destroy them.

It took over three years of contentious litigation, several Congressional investigations, and ultimately a change in presidential administration to put an end to Operation Choke Point's campaign against American business.

DOJ Forcing Banks to Terminate the Accounts of Porn Stars?, VICE NEWS (Apr. 27, 2014), available at https://bit.ly/3lGhyoD; Chris Morris, *Porn and Banks: Drawing a Line on Loans*, CNBC.COM (May 17, 2013), available at https://cnb.cx/3JY3253 .

[8] Email from a Counsel, Legal Division, FDIC, to Marguerite Sagatelian, Senior Counsel, Consumer Enforcement Unit, FDIC (August 28, 2013; 9:32AM), FDICHOGR00007424.

[9] Email from a Counsel, Legal Division, FDIC, to Marguerite Sagatelian, Senior Counsel, Consumer Enforcement Unit, FDIC (March 9, 2013; 2:53PM), FDICHOGR00005178.

[10] E-mail from Thomas J. Dujenski, Regional Director, Atlanta Region, Federal Deposit Insurance Corporation, to Mark Pearce, Director, Division of Consumer Protection, Federal Deposit Insurance Corporation (Nov. 27, 2012, 20:40:05), FDICHOGR00006585.

B. Operation Choke Point 2.0 and the Prudential Bank Regulators' War on the Innovation of the Blockchain.

The victims of Operation Choke Point 1.0 are thus all too familiar with what the participants in the crypto economy are now experiencing. The campaign begins with a series of vague policy pronouncements and ominous warnings issued in the form of informal guidance to the banks. Then there is a flurry of decisions by banks to terminate their banking relationships with the targeted industry, of accounts closed either without any explanation or with the decision being attributed to "compliance requirements," to "your business being outside of our risk tolerances," or to "risks associated with your business." As the pattern becomes apparent, there follow the Orwellian assurances from federal regulators that they "neither prohibit nor discourage banks" from doing business with any specific industries or businesses. Finally, a handful of brave and conscientious individuals at the agencies and at the banks, outraged by the abuse of the rights of their fellow Americans, come forward and bear witness to the misconduct. Past performance may not always be indicative of future results, but what the federal bank regulators have tried to get away with in the past is, it would seem, highly similar to what they are trying to get away with today.

1. The Prudential Bank Regulators Issue Informal Guidance Warning Banks of the Risks of Serving Crypto Businesses.

One of the first acts of the OCC under the Biden Administration was to kill a rule designed to "ensure fair access to banking services for several industries—including debt collection—previously cut off during the controversial Obama-era program Operation Choke Point."[11] "The Fair Access to Banking Rule emerged after what some have seen as a series of decisions by 'systemically important financial institutions (SIFIs), including Citibank, Bank of America, JP Morgan Chase … to use their market dominance to financially discriminate against legal and compliant businesses for political reasons.'"[12] It would have prohibited national banks and federal savings associations with at least $100 billion in assets from denying financial services to corporate entities, businesses, nonprofits, or individuals solely on a "subjective basis" and would set standards to impartially evaluate customer risk.[13] The rule, was finalized on January 14, 2021, after being subjected notice and comment rulemaking, and was to take effect on April 1, 2021.[14] On January 28, 2021, the Biden OCC announced that it had paused publication of the rule in the

---

[11] "Ending Operation Choke Point: Fair Access to Banking Services Addressed in Proposed Rule," *ACA International* (Nov. 22, 2020), available at https://bit.ly/3njOzaX

[12] M. Maureen Murphy," Office of the Comptroller of the Currency's Fair Access to Financial Services Rule," *Congressional Research Service: Legal Sidebar* (Feb. 5, 2021), available at https://bit.ly/3K9UNDg.

[13] *Id*.

[14] OCC News Release 2021-8, "OCC Finalizes Rule Requiring Large Banks to Provide Fair Access to Bank Services, Capital, and Credit" (Jan. 14, 2021), available at https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-8.html.

Federal Register.[15] Just seven days after taking office, therefore, the Biden OCC had suspended a rule specifically designed to guard against the resumption of Operation Choke Point.

On May 7, 2021, Secretary of the Treasury Janet Yellen appointed Michael J. Hsu as a Deputy Comptroller and announced that he would serve as Acting Comptroller of the Currency.[16] **As Mr. Hsu's subsequent statements stigmatizing the crypto industry have demonstrated, the Biden Administration had selected a self-proclaimed "crypto skeptic,"** who sees crypto and digital assets as dependent on "hype" and promoting " 'innovation' for innovation's sake,'"[17] to lead the regulation of U.S. national banks. Mr. Hsu has proven a staunch foe of the digital economy, committed "to requir[ing] that blockchain-based activities, such as stablecoin issuance, be conducted in a standalone bank-chartered entity, separate from any other insured depository institution (IDI) subsidiary and other regulated affiliates." In other words, Mr. Hsu apparently believes that crypto and crypto-banks should be choked off from the national banking system.[18]

On November 18, 2021, the OCC fired the first shot in Operation Choke Point 2.0, issuing informal guidance documents that curtailed the authority of banks to engage in cryptocurrency activities—authority that had been recognized under earlier guidance issued in 2020 and earlier in

---

[15] OCC News Release 2021-14, "OCC Puts Hold On Fair Access Rule (January 28, 2021), available at https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-14.html.

[16] Press Releases, "Secretary Yellen Announces Intention to Appoint Michael J. Hsu as First Deputy Comptroller of the Office of the Comptroller of the Currency" (May 7, 2021), available at https://home.treasury.gov/news/press-releases/jy0167.

[17] Remarks of Acting Comptroller Michael J. Hsu at the DC Blockchain Summit 2022: "Crypto: A Call to Reset and Recalibrate" (May 25, 2022), available at Acting Comptroller Michael J. Hsu remarks at the DC Blockchain Summit 2022 - Crypto: A Call to Reset and Recalibrate (occ.gov).

[18] Remarks of Acting Comptroller of the Currency Michael J. Hsu before the Institute of International Economic Law at Georgetown University Law Center: "Thoughts on the Architecture of Stablecoins" (April 8, 2022), available at Acting Comptroller of the Currency Michael J. Hsu Remarks Before the Institute of International Economic Law at Georgetown University Law Center "“Thoughts on the Architecture of Stablecoins” on April 8, 2022 (occ.gov).

2021[19]—and also limited the OCC's authority, recognized in Interpretive Letter 1176,[20] to charter a national trust bank involved in cryptocurrency-related activities.[21] Interpretive letter 1179 announced that, before engaging in any cryptocurrency activities, a bank must now notify its supervisory office, in writing, of the proposed activities and must receive written notification of the supervisory non-objection.[22] Banks that had not yet engaged in cryptocurrency activities were instructed to refrain from doing so until they received notice of supervisory non-objection from the OCC; those banks that had already commenced cryptocurrency activities were not required to discontinue those activities, but would now be obliged to notify their supervisory office.[23] Finally, the letter notes that all OCC-regulated banks should expect their cryptocurrency activities to be reviewed as part of the ongoing supervisory process.[24]

On April 7, 2022, the FDIC joined the campaign in earnest, issuing a financial institution letter requesting that all FDIC-supervised institutions that are considering engaging in crypto-related activities to notify the FDIC of their intent and provide all necessary information that would allow the FDIC to engage with the institution regarding related risks, and that any FDIC-supervised institution already engaged in crypto-related activities promptly notify the

---

[19] Specifically, Interpretive Letter 1170, had announced that banks could provide custodial services for cryptocurrencies as a modern form of traditional bank custodial and safekeeping services, noting "that providing cryptocurrency custody services is a permissible form of a traditional banking activity that banks are authorized to perform via electronic means." OCC, Interpretive Letter 1170 (July 22, 2020), available at Interpretive Letter 1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (occ.gov). Interpretive Letter 1172 had concluded that banks may hold deposits serving as reserves for stablecoins that are "backed on a 1:1 basis by a single fiat currency where the bank verifies at least daily that reserve account balances are always equal to or greater than the number of the issuer's outstanding stablecoins" and that are and held in hosted wallets under banks' existing authority to receive deposits. OCC, Interpretive Letter 1174 (Sept. 21, 2020), Interpretive Letter #1172 OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves. Finally, Interpretive Letter 1174 had concluded that national banks "may use new technologies, including INVNs and related stablecoins, to perform bank-permissible functions, such as payment activities." OCC, Interpretive Letter 1174 (Jan. 4, 2021), Microsoft Word - Interpretive Letter #1174 -Crypto 1 INVN Stablecoin Letter (occ.gov).

[20] Interpretive Letter 1176 (Jan. 11, 2021), available at Interpretive Letter 1176 (occ.gov).

[21] Interpretive Letter 1179 (November 18, 2021), available at Interpretive Letter 1179 (occ.gov).

[22] *Id.* at 1.

[23] *Id.* at 2 n.3.

[24] *Id.*

FDIC.[25] These institutions were also encouraged to notify their state regulators.[26] The FIL warned that crypto–related activities may pose significant safety and soundness and compliance risks, raise financial stability concerns, and present risks to consumers.[27]

On January 3, 2023, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency released a joint statement informing banks that the three agencies had "safety and soundness concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector."[28] The policy statement contains a series of anodyne platitudes about safety and soundness, encouraging the banks to be aware of the "risk of fraud and scams among crypto-asset sector participants" and of "inaccurate or misleading representations and disclosures by crypto-asset companies."

These warnings are, of course, as true for crypto currencies as they are for cash, gold coins, and credit cards, for mortgages and car loans, for foreign exchange and Internet commerce. If the regulators wished to ensure that these types of risks were managed properly, then they would provide guidance on how to properly manage them across all of these contexts. But instead, the regulators have chosen to single out one set of bank customers and signal that they expect banks to subject those customers to special scrutiny. Like the guidance documents issued by the agencies during Operation Choke Point, this has nothing to do with managing specific risks, and everything to do with steering clear of specific customers.

Later in the same month, the Federal Reserve issued a policy statement that discouraged banks from holding crypto assets, putting state banks on notice that "legal permissibility is a necessary, but not sufficient, condition to establish that a state member bank may engage in a particular activity."[29] Even though providing banking services to crypto companies is not prohibited by law, in other words, that does not mean that serving these customers is not prohibited by your regulator. Days later, and without public comment, the statement was entered into the Federal Register as a final rule.[30]

On February 23, 2023, the three federal banking agencies issued a second joint statement warning banks of potentially heightened liquidity risks presented by the crypto industry: some deposits by crypto companies may be subject to sudden withdrawals should the customers of those companies decide in tandem to use those deposits to buy cryptocurrencies; some deposits may represent stable-coin reserves that may need to be withdrawn should market fluctuations result in

---

[25] FDIC: FIL-16-2022: Notification of Engaging in Crypto-Related Activities

[26] *Id.*

[27] *Id.*

[28] Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), available at https://bit.ly/3TSfhDP.

[29] Policy Statement on Section 9(13) of the Federal Reserve Act, Bd. of Gov. of the Fed. Reserve Sys. (Feb. 7, 2023), available at https://bit.ly/42xegop.

[30] *Id.*

unanticipated stable-coin redemptions. One questions whether these concerns about liquidity risk—which did not materialize in 2022, even as Bitcoin *alone* declined by 65%, resulting in a $2 trillion decline in the market capitalization of that *one* cryptocurrency—are misplaced. Indeed, as the turmoil of the past few weeks has confirmed, banks would appear to face far less liquidity risk from serving crypto-customers than they do from holding long-dated U.S. Treasury securities or uninsured deposits. But what is beyond dispute is that these are risks and warnings that should apply to *any* line of business or commerce—from stockbrokers, homebuilders, automakers, and airlines to hospitals, doctors, drug companies, and military contractors—that may need to access their deposits quickly during an economic disruption, a health crisis, or a national emergency. Why, then, does the Guidance not speak to the risk that all bank customers pose, rather than singling out only those customers in the crypto industry?

As with the guidance issued as part of Operation Choke Point 1.0, all of these recent guidance documents contain the proviso that "Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type." But this assurance once again rings hollow, given that these documents name customers of only one specific class and type. Internal bank compliance officers get the message loud and clear. Imagine that the one class of customer singled out by the bank regulators were not crypto-companies, but women applying for consumer credit, or minority-owned businesses taking out commercial loans, or first-generation immigrants applying for home mortgage loans. Would such a boilerplate disclaimer transform a warning to consider credit risk, or reputation risk, or liquidity risk when lending to that group into an entirely unobjectionable statement about risk that left banks perfectly free to choose their customers? Obviously not; and just as obviously, the stigma caused by urging banks to single out and discriminate against customers in the cryptocurrency space is not cured by the disingenuous disclaimer appended to the stigmatizing guidance documents.

2. The Banks Feel the Pressure to Refuse to Accept New Crypto Customers and to Drop Crypto Customers.

While the evidence of backroom coercion is only beginning to emerge, cryptocurrency businesses are experiencing exactly what gun owners, pawn shops, and payday lenders experienced in 2012 and 2013 during the opening months of Operation Choke Point. **First, Crypto businesses are being systematically and methodically cut off from the ACH network**, as their third-party payment processors announce one-by-one that they will no longer be providing service to cryptocurrency businesses. Recently, for example, a key third party payments processor for the crypto industry, Circle, announced that it had "made the decision to stop processing ACH and wire payments for all of their partner companies…."[31]

Banks are also reportedly being pressured to limit or terminate their banking relationships with companies in the crypto industry. In August 2022, Senator Pat Toomey revealed that whistleblowers had informed him that the FDIC had instructed its regional offices to

[31] *Important Update Regarding Payment Methods*, DAPPER (last visited Mar. 23, 2023), available at https://bit.ly/3K2zK5k.

send letters to banks to discourage them from doing business with crypto companies. As Senator Toomey described the accusations to Chairman Gruenberg:

> According to whistleblower communications that we have corroborated, personnel in the FDIC's Washington, D.C. headquarters are urging FDIC regional offices to send letters to multiple banks requesting that they refrain from expanding relationships with crypto-related companies, without providing any legal basis for sending such letters. … Whistleblower reports have also alleged that the FDIC may be abusing its supervisory powers to deter banks from extending credit to crypto-related companies. According to these reports, FDIC headquarters employees have contacted FDIC regional office bank examination staff to question their review of a loan made by a bank to a crypto-related company and to urge them to downgrade their classification of the loan.[32]

Senator Toomey was clear that "[g]iven the FDIC's involvement under your leadership in the Obama administration's notorious Operation Choke Point, which sought to coerce banks into denying services to legal yet politically disfavored businesses, it is important to better understand the actions the FDIC is now taking and the legal basis for them."[33]

As a result of these pressure tactics, it is becoming harder and harder for crypto companies to obtain and maintain banking relationships. And while "some banks continue to open accounts for crypto companies, some in the industry speculated that regulators will try to cut off bank access."[34] "Operation Chokepoint 2.0 might have overplayed its hand this time," the official Twitter account for the trading Platform Kraken announced on March 12, 2023, "but the threat remains. They will continue to attack the rails, products and companies facilitating direct crypto ownership and DeFi use."[35]

Operation Choke Point 2.0 is targeting not only digital asset businesses, but also the personal accounts of individual employees of crypto businesses for termination. Just as Operation Choke Point targeted the owners and employees of the disfavored businesses, so too

---

[32] Letter from Senator Patrick Toomey, Committee on Banking, Housing, and Urban Affairs to Martin Gruenberg, Director and Acting Chairman, Federal Deposit Insurance Company (August 16, 2022), available at https://bit.ly/3Zc55Hd.

[33] Letter from Senator Patrick Toomey, Committee on Banking, Housing, and Urban Affairs to Martin Gruenberg, Director and Acting Chairman, Federal Deposit Insurance Company (August 16, 2022), available at https://bit.ly/3Zc55Hd. See also Claire Williams, *Toomey questions FDIC over 'Choke Point'-esque crackdown on banks and crypto*, AM. BANKER (Aug. 16, 2022), available at https://bit.ly/42rcc18.

[34] Joe Light, *Crypto is Being De-Banked. What It Means for Bitcoin and the Industry*, BARRONS (Mar. 13, 2023), available at https://bit.ly/42terkJ.

[35] Kraken Exchange (@krakenfx), TWITTER (Mar. 12, 2023, 10:48 PM), https://bit.ly/3Z9IUBi.

Operation Choke Point 2.0 is now targeting the men and women who work in the crypto industry. In January 2022, for example, Hayden Adams, the CEO and founder of Uniswap, a popular decentralized exchange, revealed that J.P. Morgan Chase had closed his personal bank accounts "with no notice or explanation."[36] Mr. Adams further revealed that he knew "many individuals and companies who have been similarly targeted simply for working in the crypto industry."[37] Swan Bitcoin CEO Cory Klippsten revealed that, in late 2022, Citigroup had shut down both his company's and his personal accounts without explanation. And several banks have pulled back on their exposure to the asset class.[38] While the banks have been unwilling to offer any explanation for their actions, the former Commodity Futures Trading Commissioner Brian Quintenz was clear that the move was likely an instance of shadow de-banking of crypto by Federal Reserve and OCC bank examiners.[39]

The Biden Administration's anti-crypto crusade has not been limited to the federal bank regulators. The Securities and Exchange Commission has opened a second front, targeting both the banks that serve as the custodians of digital assets and the issuers of crypto-currencies and other digital assets including stablecoins. **On April 11, 2022, the Commission issued Staff Accounting Bulletin No. 121,** which instructed those entities required to file reports under Sections 13(a) or 15(d) of the Exchange Act that they must include digital assets held in custody among the assets and liabilities on their balance sheets.[40] In contrast, conventional assets do not appear on the custodian bank's balance sheet, because those assets are recognized as belonging to the bank's clients, not the bank. This raises series questions regarding how custodianship of digital assets could impact a bank's balance sheet risk for purposes of its Basel III capital requirements.[41] By imposing this requirement, the SEC effectively placed a sword of Damocles over the head of any bank considering acting as a custodian of digital assets.

Finally, after having repeatedly invited the industry to "come in and talk with us," and many firms having done so the SEC nonetheless embarked on an aggressive regulatory and

---

[36] hayden.eth (@haydenzadams), TWITTER (Jan. 23, 2023, 11:52 AM), available at https://bit.ly/3yYScFB.

[37] *Id.*

[38] Declan Harty, "Crypto industry poised for clash with government over crackdown," *PoliticoPro* (Mar. 24, 2023).

[39] Brian Quintenz (@BrianQuintenz), TWITTER (Jan. 23, 2023, 2:10 PM), https://bit.ly/40gXqJ6 ("Likely a shadow de-banking of crypto by @federalreserve or @USOCC bank examiners, with direction from the top. If the examiner told a bank that a certain customer is too risky and the bank ended that relationship, the bank is contractually prevented from telling that customer why.")

[40] Securities and Exchange Commission, Staff Accounting Bulletin No. 121 (Apr. 11, 2022), available at SEC.gov | Staff Accounting Bulletin No. 121.

[41] "SEC crypto custody accounting rule: a serious blow for bank custodians?" *Ledger Insights* (Apr. 1, 2022), available at SEC crypto custody accounting rule: a serious blow for bank custodians? - Ledger Insights - blockchain for enterprise.

enforcement campaign against the digital asset industry. In December 2020, the SEC filed a lawsuit against cryptocurrency platform Ripple , its CEO, and its chairman, for illegally selling unregistered securities worth $1.3 billion.[42] The following March, the Commission brought an enforcement action against LBRY, claiming that its unregistered offerings of LBC violate sections 5(a) and (c) of the Securities Act.[43] On February 12, 2023, the Commission issued a Wells notice to Paxos Trust Co. announcing that it plans to sue the company for violating investor protection laws by issuing a stablecoin that the SEC claims is an unregistered security.[44] On March 22, 2023, after meeting with the SEC more than 30 times in nine months, Coinbase received a Wells notice from the Commission regarding "regarding an unspecified portion of our listed digital assets, our staking service Coinbase Earn, Coinbase Prime, and Coinbase Wallet."[45] "We asked the SEC for reasonable crypto rules for Americans," Coinbase responded: "We got legal threats instead."[46]

3. Shuttering banks that serve crypto.

The primary stick wielded by the agents of Operation Choke Point was the threat of unending audits and examinations: that federal and state regulators would smother the bank in red tape if the bank did not agree to smother its own customers. But a far more menacing threat was implicit in the statements and actions of the examiners. The banks knew that their regulators have the power to shutter any bank that refuses to bend the knee and toe the line from Washington. In one instance, when a bank expressed reluctance to terminate a longstanding and law-abiding customer simply because that customer was disliked by the bank's regulators, this implicit threat was made explicit when the head examiner openly threatened that the FDIC was simply not

---

[42] *See* Complaint, *Securities and Exchange Commmission v. Ripple Labs, Inc. et al*., ECF No. 1, Case No. 1:20-cv-10832 (S.D.N.Y. Dec. 22, 2020).

[43] *See* Complaint, *Securities and Exchange Commission v. LBRY, Inc.,* ECF No.1, Case No. 1:21-cv-00260-PB (D.N.H. March 29, 2021).

[44] Vicky Ge Huang, Patricia Kowsmann, and Dave Michaels, "Crypto Firm Paxos Faces SEC Lawsuit Over Binance USD Toke: The agency has been intensifying its enforcement of major crypto players," *WSJ* (Feb. 12, 2023), available at Crypto Firm Paxos Faces SEC Lawsuit Over Binance USD Token - WSJ.

[45] Paul Grewal, "We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead. Coinbase.com (March 22, 2023), available at We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead. (coinbase.com) On the same day, the Commission also announced that it would sue Justin Sun, the creator of the Tron cryptocurrency ecosystem, accusing him of illegally selling crypto securities and conspiring to artificially inflate trading volume in crypto assets. Press Release, SEC Charges Crypto Entrepreneur Justin Sun and his Companies for Fraud and Other Securities Law Violations (Mar. 22, 2023), available at SEC.gov | SEC Charges Crypto Entrepreneur Justin Sun and his Companies for Fraud and Other Securities Law Violations. The Commission simultaneously charged eight celebrities for illegally touting these cryptocurrencies.

[46] Paul Grewal, "We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead. Coinbase.com (March 22, 2023), available at We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead. (coinbase.com)

concerned if a "piss ant, $200 million bank failed."[47] The prudential bank regulators, in other words, have more potent weapons than harassing banks with audits and visitations.

There is reason to fear that this weapon has now been fired and that bank regulators have placed a solvent financial institution into receivership to punish it for failing to toe the administration line on crypto. On March 8, 2023, Silvergate Bank, which served as one of the two main banks offering real time ledgering for crypto companies, through its "SEN" network, announced that it would be winding down operations "[i]n light of recent industry and regulatory developments."[48] Five days later, New York State bank regulators ordered the closure of Signature Bank. Signature was the other main bank offering 24/7/365 ledgering capabilities for the digital asset companies. It was founded in 2001 as a more business-friendly alternative to the big banks. In 2018, Signature began to serve customers in the cryptocurrency industry. It created a 24/7 payments network for its crypto clients and had $16.5 billion in deposits from digital-asset-related customers. In the wake of the collapse of Silicon Valley Bank, Signature had experienced $10 billion of withdrawals on Friday, March 10.[49] But by Sunday, management had shored up the bank's capital situation, the deposit exodus had slowed, and the situation had stabilized.[50]

Nonetheless, the regulators moved in, summarily removed management, shuttered the bank, and began conducting a sale of the bank's assets. The move was suspicious. At that same time they closed Signature, the bank's regulators were moving to shore up the finances of other banks, including First Republic, that were in far more dire straits than Signature. Signature, after all, had $110.36 billion of assets to cover $88.59 billion of deposits at the end of 2022,[51] and the regulators had conceded that the bank was not insolvent at the time it was closed.[52] **The New York Department of Financial Services Superintendent, Adrienne A. Harris, also sits on the Financial Stability Oversight Council, and would surely have been well aware that the FSOC**

---

[47] OFFICE OF INSPECTOR GENERAL, REPORT NO. OIG-16-001, REPORT OF INQUIRY INTO THE FDIC'S SUPERVISORY APPROACH TO REFUND ANTICIPATION LOANS AND THE INVOLVEMENT OF FDIC LEADERSHIP AND PERSONNEL 70 (Feb. 2016), available at https://goo.gl/fjR8JH.

[48] Press Release, "Silvergate Capital Corporation Announces Intent to Wind Down Operations and Voluntarily Liquidate Silvergate Bank" (Mar. 8, 2023), available at https://ir.silvergate.com/news/news-details/2023/Silvergate-Capital-Corporation-Announces-Intent-to-Wind-Down-Operations-and-Voluntarily-Liquidate-Silvergate-Bank/default.aspx). See also MacKenzie Sigalos, "Crypto-focused bank Silvergate is shutting operations and liquidating after market meltdown" (Mar. 8, 2023).

[49] Hugh Son, *Why regulators seized Signature Bank in third-biggest bank failure in U.S. history*, CNBC (Mar. 13, 2023), available at https://cnb.cx/3Z8ZtgW.

[50] *Id*.

[51] *Id*.

[52] *Id*.

liquidity program would have obviated any risk of Signature's failure.[53] There was essentially no need for regulatory intervention.

Signature had, however, been the first FDIC-insured bank to enable its commercial clients to access a blockchain-based, real-time payments platform. Signature launched Signet in January of 2019 and, in 2020, integrated the service with digital asset custodian Fireblocks to facilitate the secure movement, storage, and issuance of digital assets.[54] At the time Signature was closed, Signet was the only 24/7 cryptocurrency bank ledgering platform, a fact that would have made Signature an appealing target for Operation Choke Point 2.0.[55]

Former Representative Barney Frank, a principal author of the Dodd-Frank legislation enacted in the wake of the 2008 financial crisis and a member of Signature's Board of Directors, agreed that there was "no real objective reason" for the bank's seizure and drew the conclusion that the bank was likely closed because of Operation Choke Point 2.0.[56] The pretext offered by regulators, i.e., that they wanted more complete data from the bank, simply did not justify the draconian action of shuttering the bank and liquidating its assets; even though it was doing crypto responsibly, the bank was shuttered because its regulators do not want banks doing crypto at all:

> Now, the question is, why did they react so harshly to what they said was our inability to give them the sufficient data? I believe it was probably to send the message that even though we were doing crypto stuff responsibly, they don't want banks doing crypto. They denied that in their statement, but I don't fully believe that. I think that they overreacted to what they saw was our problem with data, which may well have existed, but the data was improving. I think sloppy data is not a reason to close a bank that you have not decided was insolvent, and they've never said we were insolvent.

Representative Frank concluded that "part of what happened was that regulators wanted to send a very strong anti-crypto message," and Signature "became the poster boy because there was no insolvency based on the fundamentals."[57] Signature was closed to send an unambiguous message to the other banks:

---

[53] CSBS, Press Release, State Bank Supervisors Appoint New York Superintendent Adrienne A. Harris to FSOC (Dec. 13, 2022), available at [State Bank Supervisors Appoint New York Superintendent Adrienne A. Harris to FSOC | CSBS]

[54] Press Release, Signature Bank Launches its Digital Payment Platform, Signet, on the Fireblocks Network, Signature Bank (June 23, 2020), available at https://bit.ly/40rsGoc.

[55] Frederick Munawa, *Signature Bank's Signet Platform Still Works, but Some Clients Have Moved On*, COINDESK (Mar. 14, 2023), available at https://bit.ly/3LHcyeh.

[56] Hugh Son, *Why regulators seized Signature Bank in third-biggest bank failure in U.S. history*, CNBC (Mar. 13, 2023), available at https://cnb.cx/3Z8ZtgW.

[57] *Id*.

> No, I don't think they have to [begin a larger crackdown on crypto]. I think that there's already a retreat by banks from crypto. There's an old French expression — they were interested in the 18th century, how strict the discipline was in the British Navy, and in one case, the British Navy executed a guy for a relatively minor infraction because they were worried about the behavior of all the sailors. And the French said, "Oh, those peculiar English. They shoot one man to encourage the others." And that phrase, *pour encourager les autres*, people understand what that means. And I think it's probably working.

The FDIC had shown it was willing to destroy a "piss ant, $200 million bank" to signal its commitment to harming payday lenders; that the regulators were willing to precipitate the second largest bank failure in American history would send a message that is unmistakable and powerful, a message that banks ignore only at their extreme peril.

FDIC, it has been widely reported, continued to send this anti-crypto message as it wound down Signature. According to two anonymous sources, the FDIC required bidders for Signature to agree not to bid for the bank's assets with ties to the crypto industry.[58] An FDIC spokesperson denied these allegations, claiming that the agency would not require divestment of crypto activities as part of any sale, and referred concerned banks to prior statements by FDIC Chairman Martin Gruenberg that they are "neither prohibited nor discouraged" from providing services to any sector of the economy.[59]

These denials were all too familiar to the victims of Operation Choke Point, who were similarly assured by Chairman Gruenberg in 2015—indeed, in the very same words Chairman Gruenberg continues to use in 2023—that supervised banks were "neither prohibited nor discouraged from providing services to any category of business customers or individual

---

[58] David French and Pete Schroeder, *Exclusive-U.S. regulator eyes Friday bids for SVB, Signature Bank – sources*, REUTERS (Mar. 15, 2023), available at https://bit.ly/40rCiPR("The two sources added that any buyer of Signature must agree to give up all the crypto business at the bank."). See also Cheyenne Ligon, *Signature Bank's Prospective Buyers Must Agree to Give Up All Crypto Business: Reuters*, COINDESK (Mar. 16, 2023), available at https://bit.ly/40tXxQZ ("Many in the crypto industry – including former acting Comptroller of the Currency, and one-time Binance.US CEO, Brian Brooks – have speculated the closure of the three banks is indicative of a coordinated effort by regulators to choke the crypto industry off from the banking system.").

[59] Nikhilesh De, *FDIC Denies Report Signature Bank Purchaser Must Divest Crypto*, COINDESK (Mar. 16, 2023), available at https://bit.ly/3lBz6T4. See also Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities (Feb. 23, 2023), available at https://bit.ly/3FJ7QbS ("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.")

customers."[60] It thus came as no surprise when the FDIC announced on March 19, 2023, that the winning bidder for the assets of Signature Bank would not be acquiring the firm's digital asset business, "SIGNET":

> Depositors of Signature Bridge Bank, N.A., other than depositors related to the digital banking business, will automatically become depositors of the assuming institution. All deposits assumed by Flagstar Bank, N.A., will continue to be insured by the FDIC up to the insurance limit. Flagstar Bank's bid did not include approximately $4 billion of deposits related to the former Signature Bank's digital banking business. The FDIC will provide these deposits directly to customers whose accounts are associated with the digital banking business.[61]

In spite of its strenuous denials, therefore, the FDIC had in fact not been seeking to sell SIGNET and Signature's other digital assets. This decision resulted in a $2.5 billion hit to the FDIC's deposit insurance fund; the deal nevertheless closed just a week after the bank was closed, and, remarkably, was approved by regulators within one day.[62] Clearly, "the FDIC seemed to be in a hurry to close this one on terms very favorable to NYCB," Flagstar's parent.[63] As the editors of the Wall Street Journal opined, the action taken by the FDIC "confirms Mr. Frank's suspicions—and ours—that Signature's seizure was motivated by regulator's hostility toward crypto."[64]

This crackdown on crypto is not only harming bank customers, but also is a violation of the FDIC's statutory obligations to wind-down failing banks in the way that "is the least

---

[60] FDIC, Financial Institution Letter, FIL-52-2015, "FDIC Clarifying its Approach to Banks Offering Products and Services, such as Deposit Accounts and Extensions of Credit, to Non-Bank Payday Lenders" (Nov. 16, 2015), available at FDIC: Inactive FIL-52-2015: FDIC Clarifying Its Approach to Banks Offering Products and Services, Such as Deposit Accounts and Extensions of Credit, to Non-Bank Payday Lenders.

[61] Press Release, Subsidiary of New York Community Bancorp, Inc., to Assume Deposits of Signature Bridge Bank, N.A., From the FDIC, FDIC (Mar. 19, 2023), available at https://bit.ly/40hdfzu.

[62] Emily Mason, *"Signature Bank's Quick Sale Leaves Crypto Customers In The Lurch, FDIC $2.5 Billion Poorer*," *Forbes* (Mar. 22, 2023) ("It would be nice for someone to explain to the public how they are spending that $2.5 billion in just one week," Owen Lau, an analyst covering exchanges and asset managers for Oppenheimer, says. "It's a stunning expense."), available at Signature Bank's Quick Sale Leaves Crypto Customers In The Lurch, FDIC $2.5 Billion Poorer (forbes.com).

[63] *Id.*

[64] Editorial, *Barney Frank Was Right About Signature Bank: The FDIC all but confirms it closed the bank over crypto*, WSJ (Mar. 21, 2023), available at https://on.wsj.com/401B2TL.

costly to the Deposit Insurance Fund."[65] Instead the FDIC is wasting the assets of the Deposit Insurance Fund and aggravating the very risks and harms to the financial system that the bank regulators are charged with mitigating.[66] In response to Operation Choke Point 2.0, crypto firms are predictably moving their accounts off-shore, to banks in Puerto Rico, Bermuda, and the Bahamas.[67] Customers are also fleeing to offshore havens. The Chokepoint crackdown has driven at least $12 billion of US Dollar Stablecoin assets from regulated and US domiciled firms into an unregulated offshore issuer.[68]

As the editors of the Journal observed, "[m]oving dollar deposits of U.S. crypto companies and their customers offshore will make them less safe and potentially more vulnerable to money laundering."[69]

> In other words, regulators are undermining their ostensible goals. Their crypto crackdown will cost other banks and their customers. The FDIC says it "estimates the cost of the failure of Signature Bank to its Deposit Insurance Fund to be approximately $2.5 billion." If Flagstar had assumed crypto deposits, there would be no need for the insurance fund to guarantee them.[70]

"As usual, financial regulators shoot first, and make others pay later."[71]

---

[65] 12 U.S.C. § 1823(a)(4)(A) ("Notwithstanding any other provision of this chapter, the Corporation may not exercise any authority under this subsection or subsection (d), (f), (h), (i), or (k) with respect to any insured depository institution unless … (ii) the total amount of the expenditures by the Corporation and obligations incurred by the Corporation (including any immediate and long-term obligation of the Corporation and any direct or contingent liability for future payment by the Corporation) in connection with the exercise of any such authority with respect to such institution is the least costly to the Deposit Insurance Fund of all possible methods for meeting the Corporation's obligation under this section."). *See also* 12 C.F.R. § 360.1.

[66] Emily Mason, *"Signature Bank's Quick Sale Leaves Crypto Customers In The Lurch, FDIC $2.5 Billion Poorer*," *Forbes* (Mar. 22, 2023) ("'It's not fair to sit there and pick winners and losers,' Greg Ohlendorf, CEO of First Community Bank and Trust, says. 'We're going to protect the deposits of the largest institutions and their customers but if my community bank were to fail, it doesn't seem like I'm going to get the same treatment. Yet I pay my fee and my check for my FDIC assessment clears every single time.'"), available at Signature Bank's Quick Sale Leaves Crypto Customers In The Lurch, FDIC $2.5 Billion Poorer (forbes.com).

[67] Editorial, *Barney Frank Was Right About Signature Bank: The FDIC all but confirms it closed the bank over crypto*, WSJ (Mar. 21, 2023), available at https://on.wsj.com/401B2TL.

[68] Vicky Ge Huang and Caitlin Ostroff, "Tether Becomes Unlikely Crypto Winner in Banking Crisis: The stablecoin's market cap has risen 10% this year," WSJ (Mar. 14, 2023), available at Tether Becomes Unlikely Crypto Winner in Banking Crisis - WSJ.

[69] *Id.*

[70] *Id.*

[71] *Id.*

4. The Federal Bank Regulators Refuse to Charter Banks that Serve the Crypto Industry.

Having decided that they will not permit banks that serve a broad base of customers to serve the crypto industry, the federal bank regulators are now taking steps to ensure that those banks that specialize in serving the crypto industry are unable to do business in the United States. This marks a reversal of the approach that at least one of the prudential bank regulators had been taking under the prior presidential administration.

The past few years have seen the rise of regulated and unregulated financial institutions that provide digital asset services. These institutions offer different products and services, including the issuance of digital tokens, facilitating tokenization of traditional assets by their customers, providing both custody services and trading platforms for their customers. Some of these institutions have avoided government oversight, others are regulated as state money transmitter service businesses and others have sought state trust charters. At least three have sought national trust charters through the OCC. Stablecoins are the most common form of digital token issued or custodied by these trust institutions. Regulated payment Stablecoins are convertible with a traditional currency, e.g., the U.S. Dollar or Euro, on a 1-to-1 basis. The issuer backs its stablecoin by holding an equivalent amount of the hard currency or, in the case of U.S. Dollar stablecoins, in cash, short duration U.S. Treasuries and allowable overnight repo collateral. Stablecoins are used for common virtual commercial transactions, whether as an onboarding or offboarding to cryptocurrency transactions or as electronic transactions of traditional payments. A fully backed and properly custodied stablecoin carries no liquidity, duration, or credit risk.

The firms that focus on the blockchain and digital assets are subject to federal and state legal and regulatory requirements. They are required to implement BSA/AML compliance programs and must satisfy the same know-your-customer requirements as traditional banks. The issuing bank must be in a know-your-customer relationship with the party who is purchasing a stablecoin issued by the bank and who is transferring money to that bank through the banking system; the redeeming bank must be in a know-your-customer relationship with the party who is sending stablecoins back to the bank for redemption and to whom that bank is transferring money in exchange for those stablecoins.

Just as physical currency handed over the counter and placed in a customer's physical wallet will subsequently be passed from person to person without the bank's knowledge, however, a stablecoin can be passed to subsequent individuals who may not be in a know-your-customer relationship with the bank. Only the redeemer, who brings the stablecoin back to the bank for redemption, needs to be known to the bank. Unlike physical currency issued by the U.S. Mint, however, stablecoins issued on the blockchain can be traced as they move in commerce. Because the blockchains record all transactions publicly and in real time, stablecoins are more readily traceable than money moving through legacy commercial and financial systems.

Regulators and law enforcement personnel can thus trace the movement of stablecoins from account to account in real time, across state and national jurisdictional lines, without the need for subpoenas or the cooperation of foreign law enforcement agencies. The Department of Justice's 2022 arrest of individuals involved in the 2016 hack of Bitfinex, a virtual currency

exchange, and its recovery of $3.6 billion in stolen cryptocurrency, confirmed that **"cryptocurrency is not a safe haven for criminals" and that DOJ "can follow money through the blockchain."[72]** Indeed, in the case of stablecoins, the issuers have made clear that they have "the ability and the right to freeze and upgrade" their U.S. Dollar stablecoins "regardless of where the USD stablecoins are being held." One stable coin permits law enforcement to freeze and wipe that stablecoin.[73] The blockchain therefore makes cryptocurrencies far less amenable to fraud, money laundering, or tax evasion than currencies.

On January 13, 2021, the Office of the Comptroller of the Currency announced that it had granted a national trust bank charter to Anchorage Digital Bank subject to the condition that Anchorage enter into an operating agreement setting forth, among other things, capital and liquidity requirements and the OCC's risk management expectations.[74] The OCC explained that bringing Anchorage into the national banking system would permit the bank to benefit from the OCC's expertise and experience while demonstrating that the National Bank Act is sufficiently flexible to accommodate innovation and new financial technologies.[75] By the end of April, two other crypto banks had been granted provisional trust charters.[76]

This marked the high-water mark of federal bank regulator's engagement with the blockchain. Over the last year and a half, the federal bank regulators have exhibited a growing unwillingness to permit banks to serve customers doing business in the crypto industry. The Federal Reserve, for example, has slow-walked applications by two special purpose depository institutions. It has not explained why it has failed to process these applications, nor has it responded to the charge that it is acting based on bias and fear rather than evidence and sound reasoning. This has led Senator Lummis to question the Fed's "lack of responsiveness":

> Mr. Powell and Ms. Brainard have said they want to promote responsible financial innovation, when Wyoming provided a perfect opportunity the Fed instead inexplicably chose to ignore its legal obligations. I want to know why but haven't received an answer.

---

[72] Department of Justice, Office of Public Affairs, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency: Government Seized $3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange" (Feb. 8, 2022), available at https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[73] David Canellis, "PAX stablecoin has backdoor for freezing and seizing cryptocurrency: Devs built them for 'LawEnforcement'", The Next Web (Sept. 20, 2018), available at https://thenextweb.com/news/stablecoin-backdoor-law-enforcement.

[74] Press Release, OCC Conditionally Approves Conversion of Anchorage Digital Bank, Office of the Comptroller of the Currency (Jan. 13, 2021), available at https://bit.ly/40yUOGd.

[75] *Id.*

[76] OCC Conditionally Approves Conversion of Protego Trust Bank | OCC

OCC Conditionally Approves Chartering of Paxos National Trust | OCC

> The Fed's lack of responsiveness is becoming a trend. Recently, the central bank thumbed its nose at Sen. Pat Toomey's request for its research into climate and equity. As the Senate considers Mr. Powell's and Ms. Brainard's nominations, they must address these concerns.[77]

"The American people expect" their federal bank regulators, Senator Lummis concluded, "to follow the law without bias or delay."[78]

The Federal Reserve has delayed resolution of the requests from state-chartered banks to access the Federal Reserve system. Wyoming-chartered Custodia Bank applied to the Federal Reserve for a master account on October 29, 2020. The Fed is required to "take final action on any application to the agency before the end of the 1-year period beginning on the date on which a completed application is received by the agency." 12 U.S.C. § 4807. After nineteen months of inaction, Custodia Bank was at last forced to bring a lawsuit seeking to compel the agency to act. On January 27, 2023, the Kansas City Federal Reserve Bank communicated that the application was denied. This decision was reached in patent violation of 12 U.S.C. § 248a, which requires that Custodia, as a state-chartered bank, be able to access all "Federal Reserve bank services."

The Biden OCC has announced that it will subject the provisional approvals granted under former Acting Comptroller of the Currency Brooks' leadership to heightened scrutiny. "Charters that were in the pipeline as well as those that were conditionally approved" are "in the scope of the review," according to Hsu.[79] "As a member of the FDIC board and of the Financial Stability Oversight Council, Hsu said 'I want to use all the seats I have' " to pursue "an overall strategy and overall view about where the regulatory perimeter should be set" for cryptocurrencies.[80]

The strategy Hsu appears to be implementing is consistent with Operation Choke Point 2.0's war on crypto. In April 2022, OCC fired a shot across the bow of Anchorage Digital Bank, issuing a consent order for Anchorage's purported failure to meet Bank Secrecy Act/anti-money laundering requirements imposed under its operating agreement with the OCC.[81] The other two national bank charters conditionally granted to crypto-banks by OCC in 2021 remain in regulatory limbo. In the case of one, Protego Trust Bank, the OCC appears to have allowed the conditional

---

[77] Cynthia Lummis, *The Fed Battles Wyoming on Cryptocurrency*, WSJ (Nov. 30, 2021), available at https://on.wsj.com/3JD6DnF.

[78] *Id*.

[79] "OCC's Hsu: Recent Approvals of Crypto Charters 'On the Table' for Review," ABA Banking Journal (June 2, 2021), available at www.bit.ly/3FQPCpg.

[80] *Id*.

[81] "OCC Issues Consent Order Against Anchorage Digital Bank," News Release 2022-41 (April 21, 2022), available at https://www.occ.gov/news-issuances/news-releases/2022/nr-occ-2022-41.html.

charter to expire on February 4, 2023. According to an OCC spokesperson, the "pre-conversion requirements included policies, procedures, systems and other measures to ensure the safe and sound operation of the bank as well as meeting minimum capital and liquidity requirements."[82] As a result, on March 1, 2023, Protego was forced to lay off most of its workforce, and wiped out the $70 million raised by Protego specifically to pursue a national trust charter.[83] It goes without saying, moreover, that since the OCC issued Interpretive Letter 1179, announcing that the path to chartering a national trust bank that is engaged in cryptoasset-related activities is far narrower than previously announced, no new national trust bank charter for a crypto-native company has been approved by the OCC.[84]

Caitlin Long of Custodia Bank reports that there is mounting evidence of coordination in the build-up to both the Fed's denial of Custodia's applications, as well as the non-approvals of the other institutions' charter applications.[85] Several leaks made in the days leading up to these decisions appear to have been made to pressure Custodia and the other banks to withdraw their applications, and thereby save the agencies from having to issue final (judicially reviewable) decisions.[86]

III. The Agencies' Backroom War Against Crypto is Unlawful and Unconstitutional, As Well As Arbitrary, and Capricious.

A. Operation Choke Point 2.0 is Unconstitutional.

1. Operation Choke Point 2.0 Violates the Due Process Clause.

Pressuring banks to drop or refuse to accept crypto customers, shuttering a bank that served crypto customers—Operation Choke Point 2.0 is following the same plan as the first version to destroy a legitimate industry by defaming participants in that industry. This violates, among other constitutional provisions, the fundamental protections of the Fifth Amendment's Due Process Clause.

Standing alone, government defamation does not violate due process. But due process is implicated when the government (1) defames (*i.e.*, stigmatizes) a person or entity, and (2) that

---

[82] Derek Anderson, "Protego's conditional national bank status expired without approval: Report," *Cointelegraph* (Mar. 17, 2023), available at https://cointelegraph.com/news/protego-s-conditional-national-bank-status-expired-without-approval-report.

[83] Ian Allison and Nikhilesh De, "Crypto Bank Charter Firm Protego Lays off Most of its Workforce: Source," CoinDesk (Mar. 1, 2023), available at [Crypto Bank Charter Firm Protego Trust Lays Off Most of Its Workforce: Source (yahoo.com)].

[84] David L. Portilla and Danjie Fang, "Cryptoasset-related Activities of Banks: An Overview of Trust Charters and the Use of M&A," *American Bar Association: Business Law Today* (Nov. 1, 2022), available at https://bit.ly/3z73TKs.

[85] Bitcoin 200T (@Bitcoin200T), TWITTER (Mar. 14, 2023, 7:29 PM), available at https://bit.ly/3z1jefv.

[86] *Id.*

stigmatization causes or is connected to an adverse impact on one of that person or entity's liberty or property rights. This sort of due-process violation can occur in two general ways, one forward-looking and the other backward-looking.

Beginning with the Supreme Court's decision in *Wisconsin v. Constantineau*, 400 U.S. 433 (1971), courts have held that due process must be afforded before the government can stigmatize a person in a way that alters his background legal rights or status. This "stigma-plus" theory is a forward-looking inquiry, asking whether stigmatizing actions or statements alter or extinguish a right, previously held, to engage in some activity in the future. Where the right in question is the right "to follow a chosen trade or profession," *Cafeteria & Rest. Workers Union, Local 473 v. McElroy*, 367 U.S. 886, 895–96 (1961), courts have more specifically asked whether the plaintiff has been "broadly precluded" from engaging in a chosen line of business. *See Trifax Corp. v. District of Columbia*, 314 F.3d 641, 645 (D.C. Cir. 2003).

A separate line of cases holds that due process must be provided where the government stigmatizes a plaintiff in the course of extinguishing the plaintiff's protected rights or benefits. This "reputation-plus" inquiry, arising from the Supreme Court's decision in *Board of Regents of State Colleges v. Roth*, 408 U.S. 564 (1972), is generally backward-looking, asking whether the government denied the plaintiff a legal entitlement and damaged his reputation at the same time.

Where the government is guilty of a stigma-plus or reputation-plus violation, the court will order it to provide adequate process, that is, a process by which the plaintiff may rebut the stigmatizing charges that caused his loss of liberty or property. The plaintiffs that challenged Operation Choke Point 1.0 brought stigma- and reputation-plus claims. And though the claims were not ultimately resolved—the case was voluntarily dismissed after the Federal Government finally ended the Operation—the U.S. District Court for the District of Columbia found a legally valid claim was stated. The background right at issue there was the right to access the banking system in common with the rest of the citizenry. The stigma came from the Government's repeated statements tarring payday lenders as "high-risk" banking customers and from its pressuring banks to drop these customers. Many banks concluded that this disfavored relationship was not worth the expense that this government hostility imposed, and they proceeded to drop or turn away payday-lending clients as demanded.

Operation Choke Point 2.0, like the previous version, raises due process concerns under both the stigma-plus and reputation-plus theories.

Stigma-plus. In *Wisconsin v. Constantineau*, 400 U.S. 433 (1971), the Supreme Court addressed a Wisconsin statute that allowed government officials to prohibit businesses from selling alcohol to certain persons through "postings" that labelled them as excessive drinkers. The chief of police had posted such notice about the plaintiff in retail liquor establishments in a particular town—effectively forcing her to drive to the next town to purchase alcohol. The Court held that the Wisconsin statute violated the Due Process Clause by allowing the government to label individuals as excessive drinkers and alter their background legal rights without providing them any procedural protections. "Where a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him," the Court explained, "notice and an opportunity to be heard are essential." *Id*. at 437.

The Court reaffirmed *Constantineau*'s central holding in *Paul v. Davis*, 424 U.S. 693 (1976). The "[p]osting" in *Constantineau*, the Court reasoned, had "deprived the individual of a right previously held under state law . . . to purchase or obtain liquor in common with the rest of the citizenry." *Id.* at 708. In that way, "a right or status previously recognized by state law was distinctly altered or extinguished," and this "alteration of legal status . . . combined with the injury resulting from the defamation . . . justified the invocation of procedural safeguards." *Id*. at 708–09, 712.

The backroom war against the crypto industry violates the Due Process Clause under the very same reasoning. Whereas *Constantineau* concerned a relatively minor burden on the right to purchase alcohol, here, as in Operation Choke Point 1.0, the background right at issue is the right to access the banking system in common with all other citizens and businesses. Indeed, the growing evidence of regulators' backroom efforts to force a general debanking of crypto clients, coupled with federal regulators' refusal to charter banks that serve the crypto industry, suggest an attempt to "broadly preclud[e]" crypto companies from existing at all, a separate and equally sufficient liberty deprivation. *See Trifax Corp.*, 314 F.3d at 645.

As in any defamation case, the plaintiff in a stigma-plus (or reputation-plus) case must show that the government "utter[ed] . . . a statement sufficiently derogatory to injure his or her reputation, that is capable of being proved false, and that he or she claims is false." *Vega v. Lantz*, 596 F.3d 77, 81 (2d Cir. 2010). Based even on the evidence that has come to light so far, that requirement is likely to be readily met. As in Operation Choke Point 1.0, regulators began with public statements raising "safety and soundness concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector." And as in Operation Choice Point 1.0, regulators appear to be using these purported "concerns" to coerce banks to drop crypto clients. Certainly, the crypto companies that find themselves on the sharp end of these tactics will claim that these statements—conveying that crypto currencies and crypto companies *in particular* raise concerns that in fact are shared by other currencies, financial instruments, and financial sectors—are false, and are capable of being proven false. In other words, regulators have effectively labeled crypto clients as high-risk just as they labeled banks' payday-lending clients as high-risk in the first Operation Choke Point. This label is akin to the "excessive drinker" label in *Constantineau*.

The label also has the effect of depriving those in the crypto industry of their legal rights. "Many people" would consider the right to "hold bank accounts" to be "more important than the right to purchase liquor" at issue in *Constantineau*, and it therefore deserves at least as much procedural protection. *See National Council of Resistance of Iran v. Department of State*, 251 F.3d 192, 204 (D.C. Cir. 2001) ("*NCRI*"). As seen, this label has deprived crypto-industry participants of the right to hold a bank account. And they received no procedural protection before being tarred in this way. They were given no notice that regulators were planning to adopt a de facto policy of stigmatizing them as high-risk and pressuring banks to terminate their business. Nor were they given any opportunity to contest the label. Shortly after the policy statements identifying purported risks in their industry, they simply, and suddenly, found themselves debanked. Due process demands more and better of the government than this.

To be sure, labeling the plaintiff as an "excessive drinker" in *Constantineau* prohibited her from purchasing alcohol in her hometown, whereas banks are not officially forbidden from allowing crypto clients to hold accounts. But due process is required before a pre-existing right is "distinctly *altered or extinguished*." *Paul*, 424 U.S. at 711 (emphasis added). In *Constantineau* itself, the burden on the plaintiff's right to purchase alcohol was relatively minor: because the state law at issue prohibited her only from purchasing alcohol in one particular town, the effect of the law was merely to make her drive to the next town to buy liquor. The Supreme Court has thus described the right at issue in *Constantineau* as the right "to purchase or obtain liquor *in common with the rest of the citizenry*," not the right to purchase or obtain liquor *at all*. *Id.* at 708 (emphasis added).

Regulators have stigmatized crypto companies by labeling them as risky banking clients, both in public statements and, the evidence suggests, in statements directly to banks. As a result, crypto companies are losing the right to maintain banking relationships and, because many will surely fail without such relationships, they face broad preclusion from operating in the industry of their choice. The government cannot stigmatize businesses and alter their background rights in this way without due process, which the government has not even arguably provided here.

Reputation-plus. The year after deciding *Constantineau*, the Supreme Court decided *Board of Regents of State Colleges v. Roth*, 408 U.S. 564 (1972). The plaintiff there (Roth), who had been a non-tenured professor at a state university in Wisconsin, was informed that he would not be rehired when his teaching contract expired. Roth argued that the decision violated his due process rights. Although the Supreme Court rejected this claim, it emphasized that it did so only because the "State, in declining to rehire the respondent, did not make any charge against him that might seriously damage his standing and associations in his community . . . . Had it done so, . . . due process would accord an opportunity to refute the charge before University officials." *Id.* at 573. As the Court later reiterated in *Paul*: "*Roth* recognized that governmental action defaming an individual in the course of declining to rehire him could entitle the person to notice and an opportunity to be heard as to the defamation." 424 U.S. at 709. Following *Roth* and *Paul*, the D.C. Circuit, like other courts, has repeatedly recognized that "defamation in the course of the termination of employment is" actionable under the Due Process Clause. *O'Donnell v. Barry*, 148 F.3d 1126, 1140 (D.C. Cir. 1998) (quotation marks omitted); *see also, e.g.*, *Lyons v. Barrett*, 851 F.2d 406, 407 (D.C. Cir. 1988).

Victims of Operation Choke Point 2.0 can also establish the elements of a reputation-plus claim. Loss of the right to a banking relationship is akin to the loss of government employment. *See NCRI*, 251 F.3d at 204 (due process implicated where the government impaired the "right to . . . hold bank accounts"); *Old Dominion Dairy Prods., Inc. v. Secretary of Defense*, 631 F.2d 953, 964 (D.C. Cir. 1980) (extending reasoning of *Roth* to reach denial of government contracts, explaining that to "rule otherwise would drain *Roth* of meaning"). And these terminations have occurred against the backdrop of the government's false claims that serving crypto clients—and crypto clients uniquely—threatens the safety and soundness of banks.

As described above, these debanking efforts appear to be an attempt to broadly preclude crypto companies from doing business as crypto companies. Like the stigma-plus theory, however,

the reputation-plus theory would not require a crypto company to show that it have been cut off from the banking system entirely. Rather, the company would only need to show defamation "in the course of the termination" of its bank accounts. *See O'Donnell*, 148 F.3d at 1140; *see also Owen v. City of Independence, Mo.*, 445 U.S. 622, 633 n.13 (1980). To be sure, it would also need to show a relationship between these terminations and regulators' actions—that is what makes the loss of bank accounts equivalent to the loss of government employment in other reputation-plus cases. But the existing evidence already strongly suggests if not proves that regulators caused these terminations by making false statements about the riskiness of crypto clients and then using such statements to pressure banks to drop them.

2. Operation Choke Point 2.0 May Violate Structural Constitutional Protections.

The regulators' attempt to strangle the entire crypto industry also may run afoul of the non-delegation doctrine. "The nondelegation doctrine bars Congress from transferring its legislative power to another branch of Government." *Gundy v. United States*, 139 S. Ct. 2116, 2121 (2019). If, as appears to be the case, regulators have adopted and are now enforcing a de facto policy that the crypto industry is too risky to be banked (and therefore to exist), then regulators have exercised legislative power.). Indeed, they have acted as the judge, jury, and executioner of American businesses, the greatest threat to liberty that the Founders could conceive. *See Gundy*, 139 S. Ct. at 2133–35 (Gorsuch, J., dissenting). Here, for the reasons below, regulators could not show that Congress *did* delegate them the authority to adopt this anti-crypto policy. But even if the applicable statutes could be construed in that way, regulators' exercise of that purported authority would violate the nondelegation doctrine.

To be sure, though attention to the nondelegation doctrine has been revived, the doctrine has been enforced against few federal actions to date. But the remedy for federal actions that violate this doctrine would be to enjoin those legally baseless actions. And based on the facts already known, regulators have at least subjected themselves to potential litigation under this doctrine, too.

B. The Federal Bank Regulators Are Failing To Perform Their Statutory Duties.

1. The Bank Regulators are Exceeding their Statutory Authority.

The federal prudential bank regulators are charged with ensuring that law-abiding Americans have access to banks that are "safe and sound."[87] They do so not by managing the risks for the banks, but by ensuring that the banks themselves have adequate standards, practices, and procedures in place for managing risk. Section 1831p-1(a) authorizes the prudential regulators to promulgate standards relating to the risk-management systems and controls that the banks use to protect their own safety and soundness.

[87] *See* 12 U.S.C. § 1831p-1.

To be sure, the federal bank regulators are more closely engaged with the banks they supervise than are the regulators of other industries.[88] And this supervision of the banks can involve stringent evaluation of the bank's business decisions. But this supervisory authority is not plenary. The regulators are not authorized to make business decisions for the banks, much less to demand that the banks close the accounts of law-abiding customers. By seeking to coerce banks to stop doing business with specific lawful industries, the Federal Reserve, the FDIC, and the OCC have thus gone beyond their statutory authority to ensure that banks manage risk. They are making the day-to-day business decisions for the banks. The prudential bank regulators have no authority to do this.

This abuse is all the more striking given that the regulators, here, are effectively leveraging their statutory authority over the banks to set economic and technology policy for the United States economy as a whole. The blockchain is bringing changes to the global financial system that could rival those ushered in by the rise of the Internet and electronic commerce. The regulators of the nation's banks have no warrant to unilaterally wall off the American economy from these emerging changes.

2. The Federal Banking Regulators are Not Performing their Statutory Duties.

At the same time as they are usurping the role that belongs to the banks, the federal banking regulators are failing to perform the duties that are statutorily assigned to them. The Federal Reserve has failed, for example, to adjudicate the applications submitted by State-chartered banks and Special Purpose Depository Institutions to join the federal reserve system in a timely fashion. This is a clear violation of 12 U.S.C. § 4807 and the Administrative Procedure Act. Section 4807, as discussed above, requires the Fed to review applications "before the end of the 1-year period beginning on the date on which a completed application is received by the agency." 12 U.S.C. § 4807. Custodia Bank's application for a master account was denied only after 27 months had elapsed, and even then the Board issued its decision only after Custodia had brought suit in federal district court to compel it to act.

The Federal Reserves' outright denial of Custodia's application for a master account is likewise directly contrary to law**. The Federal Reserve has no discretion to deny a state-chartered depository institution's application for a master account.** Section 248a(c)(2) of Title 12 provides that "[a]ll Federal Reserve bank services covered by the fee schedule shall be available

[88] The Supreme Court memorably described this supervisory authority in *United States v. Phila. National Bank*, 374 U.S. 321, 329 (1963) ("But perhaps the most effective weapon of federal regulation of banking is the broad visitorial power of federal bank examiners. Whenever the agencies deem it necessary, they may order 'a thorough examination of all the affairs of the bank,' whether it be a member of the Federal Reserve System or a nonmember insured bank. Such examinations are frequent and intensive. In addition, the banks are required to furnish detailed periodic reports of their operations to the supervisory agencies. In this way the agencies maintain virtually a day-to-day surveillance of the American banking system. And should they discover unsound banking practices, they are equipped with a formidable array of sanctions.") (cleaned up).

to nonmember depository institutions …"[89] 12 U.S.C. § 248a(c)(2). Custodia is a state-chartered bank whose charter expressly permits U.S. dollar deposit-taking, and is thus a "nonmember depository institution[]" under the statute. Because Custodia must have a master account to access the "Federal Reserve bank services" enumerated under Section 248a, the refusal to grant it such an account is contrary to the command of Section 248a(c)(2).

The most troubling failure that has come to light so far, however, is the decision by state and federal regulators to force banks into receivership when they do not bend to the regulators' wishes. Ensuring the safety and soundness of the banks is the *raison d'etre* of federal bank regulation. An insolvent bank is placed into receivership in order to ensure that the contagion does not spread and the soundness of the financial system is protected. That a solvent financial institution may have been placed into receivership solely "*pour encourager les autres*" means that the federal regulators now appear willing to sacrifice the very safety and soundness they are charged with protecting in order to give their private biases the force of law.

C. The Prudential Bank Regulators are Violating the Administrative Procedure Act.

The prudential bank regulators' campaign against the crypto industry is not only substantively unlawful, it is procedurally defective as well. In conducting their campaign of informal regulation, surreptitious defamation, and backroom coercion, the bank regulators have violated the Administrative Procedure Act by acting beyond their statutory authority, without using the notice and comment rulemaking procedures required by law, and in an arbitrary and capricious manner.

1. The Prudential Bank Regulators Have Acted Beyond Their Statutory Authority.

By leveraging their authority over the banks to pick and choose the customers a bank may serve, the bank regulators have exceeded their statutory authority.[90] As noted above, the federal bank regulators are charged with ensuring that law-abiding Americans have access to banks that are "safe and sound."[91] They are not charged with regulating new technologies or policing the nation's economy; nor are they permitted to confer the force of law on their personal biases and prejudices. Putting aside the fundamental unfairness and the patent unconstitutionality of what these agencies are doing, there is simply no law that authorizes them to regulate the activities they are seeking to prohibit.

---

[89] The services covered by the schedule of fees are: "(1) currency and coin services; (2) check clearing and collection services; (3) wire transfer services; (4) automated clearinghouse services; (5) settlement services; (6) securities safekeeping services; (7) Federal Reserve float; and (8) any new services which the Federal Reserve System offers, including but not limited to payment services to effectuate the electronic transfer of funds." 12 U.S.C. § 248a(b).

[90] The APA requires a reviewing court to set aside agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." See 5 U.S.C. § 706(2)(C).

[91] *See* 12 U.S.C. § 1831p-1.

2. The federal bank regulators have evaded the notice and comment rulemaking requirements of the Administrative Procedure Act.

The federal agencies responsible for Operation Choke Point 2.0 have also violated the federal law that governs how agencies are to implement the laws enacted by Congress. The guidance documents and other actions decreeing who may and who may not access the financial system have all been issued without resort to any kind of formal rulemaking procedure. But the Administrative Procedure Act requires federal agencies to provide the public with notice whenever they plan to impose a binding norm and to permit the public to comment on that proposed norm before it is given the force of law.[92]

The requirements of "notice and comment" rulemaking ensure that the people know what their government is doing, while at the same time allowing the agencies themselves to benefit from the input of those who are going to be regulated, and who might be harmed, by a proposed rule. An administrative decision "can only be a well reasoned and informed decision if it is reached through the safeguard procedures established by law to ensure that result, namely, the notice and comment requirements of the APA."[93] And only "if the Agency, in carrying out its 'essentially legislative task,' has infused the administrative process with the degree of openness, explanation, and participatory democracy required by the APA, [will it] thereby have 'negate(d) the dangers of arbitrariness and irrationality in the formulation of rules.'"[94] Compliance with both the letter and the spirit of the APA's "notice and comment" rulemaking procedures is thus essential if democratic and informed government is to endure in the age of the regulatory state.

The bank regulators behind Operation Choke Point 2.0 are by no means the first federal agencies that have worked to evade the accountability inherent in the requirements of notice and comment rule-making. The mass proliferation of informal guidance has resulted in "[l]aw [being] made, without notice and comment, without public participation, and without publication in the Federal Register or the Code of Federal Regulations."[95] An agency operating through informal

---

[92] 5 U.S.C. § 553(b). The APA defines a "rule" as "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency ...." Id. § 551(4).

[93] *Housing Study Group v. Kemp*, 736 F.Supp. 321, 335 (D.D.C. 1990). *See also Chocolate Mfrs. Ass'n of the United States v. Block*, 755 F.2d 1098, 1103 (4th Cir. 1985) ("The notice-and-comment procedure encourages public participation in the administrative process and educates the agency, thereby helping to ensure informed agency decisionmaking."); *State of New Jersey, Department of Environmental Protection v. U.S. Environmental Protection Agency*, 626 F.2d 1038, 1045 (D.C. Cir. 1980) ("It is now a commonplace that notice-and-comment rule-making is a primary method of assuring that an agency's decisions will be informed and responsive.").

[94] *Weyerhaeuser Co. v. Costle*, 590 F.2d 1011, 1027-28 (D.C.Cir.1978) (*quoting Automotive Parts & Accessories Association v. Boyd*, 407 F.2d 330, 338 (D.C.Cir.1968).

[95] *Appalachian Power Co. v. EPA*, 208 F.3d 1015, 1020 (D.C. Cir. 2000) (citations and internal quotation marks omitted).

guidance more easily aggrandizes its power, moreover, by "immunizing its lawmaking from judicial review."[96]

Operation Choke Point 2.0's refusal to follow notice and comment rulemaking has produced the very result that the authors of the APA were seeking to avoid: arbitrary, capricious, and above all undemocratic agency action. The SEC's informal guidance requiring custodians to keep crypto assets on their books results in the drawing of unreasoned and unreasonable distinctions between assets held in custodianship and introduces substantial regulatory uncertainty into the Basel III regime.[97] By abandoning a final rule duly adopted after notice and comment rulemaking, and pursuing a course announced in informal guidance, the OCC has subjected provisionally chartered crypto banks to shifting standards and substantial unfairness.[98] The Federal Reserve's decision to create a rebuttable presumption that crypto poses heightened risks by issuing informal guidance on February 7, 2023, has resulted in the distinctions between national and local banks, and their respective abilities to meet the needs of customers engaged in the cryptocurrency business, being ignored by federal regulators.[99] The vague and platitudinous statements contained in the other guidance documents issued by the banking regulators do nothing but provide an opportunity for open-ended interpretations, arbitrary application, and regulatory abuse.[100] The result is that the federal regulators have established a scheme of *de facto* regulation of the blockchain that is ill-informed, ill-conceived, and capriciously executed. It has resulted in the banks not knowing what they must do to comply with the law, in regulators conferring the force of law upon their personal biases and capricious whims, and in the American people being left in the dark about what its government is saying about them in the backrooms of America's banks.

The blockchain cannot be un-invented. The role that this technology and the cryptocurrencies that it has made possible will ultimately come to play in our economy and in our democracy remain to be discovered. If the agencies behind Operation Choke Point 2.0 have their way, however, that role will be determined by uninformed regulators, acting in the shadows, subject to none of the checks and balances the authors of the Administrative Procedure Act, and the framers of the Constitution, deemed essential to sound and democratic government.

---

[96] *Id.*

[97] Securities and Exchange Commission, Staff Accounting Bulletin No. 121 (Apr. 11, 2022), available at SEC.gov | Staff Accounting Bulletin No. 121.

[98] OCC News Release 2021-14, "OCC Puts Hold On Fair Access Rule (January 28, 2021), available at https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-14.html.

[99] Policy Statement on Section 9(13) of the Federal Reserve Act, entered into the Federal Register on 7 February 2023.

[100] Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), available at https://bit.ly/3TSfhDP.

3. **The Agencies have acted arbitrarily and capriciously by denying access to the banking system to new technologies they do not understand.**

Whatever the motivation of the banking regulators in waging war against the cryptocurrency industry may be, one thing is clear: their actions are not the product of the reasoned decisionmaking that the APA requires. Instead, their actions constitute the very type of arbitrary and capricious agency action that the APA prohibits.[101]

Although the arbitrary and capricious standard is "narrow," "as courts defer to the agency's exerptise,"[102] it "is not toothless."[103] For administrative action to pass muster under the APA, an agency must "examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made."[104] This requirement includes a duty to account for relevant distinctions,[105] to treat like cases alike,[106] and to explain why Americans are being treated differently one from another.[107] "Moreover, an agency cannot fail to consider an important aspect of the problem or offer an explanation for its decision that runs counter to the evidence before it."[108]

---

[101] *See* 5 U.S.C. § 706(2)(A) (providing that a reviewing court must set aside agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law").

[102] *Center for Food Safety v. Salazar*, 898 F. Supp. 2d 130, 138 (D.D.C. 2012) (*quoting Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins.*, 463 U.S. 29, 43 (1983)).

[103] *Shawnee Tribe v. Yellen*, 483 F.Supp. 3d 36, 46 (D.D.C. 2022).

[104] *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (quotation marks omitted).

[105] *See American Trucking Ass'ns Inc. v. Federal Motor Carrier Safety Admin.*, 724 F.3d 243, 253 (D.C. Cir. 2013) (finding that an unexplained decision to apply same safety regulations to short- and long-haul drivers is arbitrary and capricious); *American Wildlands v. Norton*, 193 F. Supp. 2d 244, 256 (D.D.C.2002) (finding that failure to distinguish between threatening and benign conduct is arbitrary and capricious).

[106] *Westar Energy, Inc. v. FERC*, 473 F.3d 1239, 1241 (D.C. Cir. 2007) ("A fundamental norm of administrative procedure requires an agency to treat like cases alike. If the agency makes an exception in one case, then it must either make an exception in a similar case or point to a relevant distinction between the two cases."). See also *Consolidated Edison Company of New York v. Federal Energy Regulatory Commission*, 45 F.4th 265, 279 (D.C.Cir. 2022) (same); *Kirk v. Commissioner of Social Security Administration*, 987 F.3d 314, 321 (4th Cir. 2021) (same). Indeed, a federal agency "can be said to be at its most arbitrary" when it "treat[s] similar situations dissimilarly." *Steger v. Def. Investigative Serv. Dep't of Def.*, 717 F.2d 1402, 1406 (D.C. Cir. 1983).

[107] *See City of Mesa v. FERC*, 993 F.2d 888, 896-98 (D.C. Cir. 1993) (distinguishing regulated entities based on unexplained factors also arbitrary and capricious).

[108] *Dist. Hosp. Partners, L.P. v. Burwell*, 786 F.3d 46, 57 (D.C. Cir. 2015) (cleaned up).

Indeed, one of the leading cases addressing the contours of arbitrary and capricious review, *Camps v. Pitts*, involved a failure by the Office of the Comptroller of the Currency to articulate its reasons for denying an application for a national bank charter.[109] Although the Comptroller is not required to hold a hearing or to make formal findings on the hearing record when passing on applications for new banking authorities, he was required to offer a reasoned explanation for his decision to deny the application for a national bank charter.[110] Here it appears that the OCC committed precisely the same mistake again. Rather than respond to the filings submitted by Protego, it would appear that the OCC simply allowed Protego's conditional charter to expire without rejecting that filing or formally explaining why it deemed that filing inadequate.[111] It would appear, therefore, that the Comptroller has learned nothing in the 50 years that have intervened since the Court handed down its decision in *Pitts.*

Failure to engage in reasoned decisionmaking is the hallmark of Operation Choke Point 2.0. The regulators have articulated simply no reason why the presence of a cryptocurrency business would raise serious liquidity concerns with examiners and regulators, while a customer base consisting almost exclusively of venture capitalists and startups, the cause of the collapse of Silicon Valley Bank, or one dominated by commercial real estate developers, the cause of the fall of Signature Bank, would raise none. Why would banking crypto business raise concerns about "inaccurate or misleading representations and disclosures," but banking marijuana businesses—a line of commerce prohibited by federal law—draw a wink and a nod? **Why would the government force a solvent bank into receivership, while engineering a rescue package for a different bank that was hopelessly illiquid?** There are no apparent reasons for the distinctions being drawn or for the actions being taken by the agents of Operation Choke Point 2.0. That is the halmark of arbitrary and capricious agency action.

IV. Congress Should Perform its Duty and Rein in these Regulatory abuses.

It has been 2000 years since the Roman poet Juvenal first posed the question: Who will watch the watchmen? Today, Operation Choke Point 2.0 poses the question anew: who will supervise the supervisors of our nation's banks? In our constitutional system of checks and balances, the answer to that question is clear: Congress. And in light of the mounting evidence of persistent misconduct by our nation's financial regulators, the time to perform that role is now. There are at least five specific steps that Congress can and should take.

First, Congress should require the bank regulators to produce their communications with supervised financial institutions and with state regulatory agencies regarding the provision of banking services to customers in the crypto industry. Due process, fundamental fairness, and common sense demand that those businesses that federal regulators are labeling as risky or unsound be given an opportunity to respond to these charges and defend themselves. It is particularly important that Congress exercise this supervisory responsibility and obtain these

[109] 411 U.S. 138 (1973).

[110] 411 U.S. at 141-43.

[111] Weekly Bulletin for Period 03/05/2023-03/11/2023, OCC (last visited Mar. 23, 2023), available at https://bit.ly/3G8FQyX.

documents because in private litigation, the government is likely to try to hide behind various privileges to avoid disclosing damning evidence.

Second, Congress should require the federal bank regulatory agencies to explain the basis for their conclusion that the safety and soundness of the financial system require the insulation of the banks from blockchain technology, from customers who operate in the crypto space, and from state-chartered depository institutions that are currently serving those customers. The federal bank regulators have elected to single out a specific industry for exclusion from the banking system. If those regulators have concluded that a specific industry can never be banked in a safe and sound fashion, then the basis and the reasoning behind that decision need to be subjected to review and to scrutiny. The Agencies should be required to explain whether their obsessive focus on campaigning against crypto diverted their resources away from the broad and systemic risks that were growing in the financial system and that have contributed to the current loss of confidence in the banking system.

Third, Congress should make clear to the federal bank regulators that the notice and comment rulemaking requirements of the Administrative Procedure Act are not optional. These protections were put in place to promote informed, reasoned, and democratic decisionmaking by all federal agencies, including the prudential bank regulators. Final agency actions are likewise subject to judicial review to ensure that the agencies have done their jobs and to preserve our system of checks and balances in the administrative state. The requirements imposed by the APA are not obstacles to evaded by improper reliance on informal guidance documents. The Federal bank regulators should be made to explain their decision to forego seeking input from experts and industry participants through notice and comment rulemaking and to rely instead exclusively on informal guidance when regulating this new technology.

Fourth, Congress should require FDIC to reveal whether any banks responded to its April 7, 2022, Guidance requesting that they inform the Corporation if they are considering engaging in crypto-related activities, that they provide all necessary information that the FDIC would need to engage with the institution regarding related risks, and that any FDIC-supervised institution already engaged in crypto-related activities promptly notify the FDIC. Congress should require FDIC to explain how it responded to these requests, and whether any of these banks were discouraged from engaging in crypto-related activities.

Fifth, Congress should investigate the role of federal regulators in the decision by the New York Department of Financial Supervision to shutter Signature Bank. It should require production of communications between federal regulators and officials and New York State regulators and officials, including New York Department of Financial Services Superintendent Adrienne A. Harris, related not only to the closure of Signature Bank, but to the coordination of efforts to limit bank participation in crypto-related activities. The American people need to know what role, if any, federal regulators played in the decision by New York's regulators to place Signature into receivership. They deserve to know whether this bank was allowed to fail because of its financial condition, or forced to fail, in spite of its soundness, because of its customers. Furthermore, the FDIC needs to come clean on whether it encouraged or required banks that sought to bid on the assets of Signature Bank to exclude the digital assets of Signature from their bids. And if the FDIC

in fact received bids that would have covered those assets, then it needs to explain why it selected a bid that left the FDIC on the hook for those digital deposits and cost Signature's digital asset team their jobs.

Sixth, Congress should require the bank regulatory agencies to explain why First Republic Bank and PacWest, which had no exposure to crypto-activities but were in a worse financial position than Signature, were given an opportunity to save themselves, while Signature was given neither time nor opportunity to seek needed liquidity.

Finally, Congress should investigate whether bank regulators are acting to curtail private sector innovation to clear the field of competition for a federal cryptocurrency alternative. Clearly, a decision to restrict the use of blockchain technology by private companies so that the technology may be reserved for the agents of the federal bureaucracy is the sort of major policy decision that the elected representatives of the people assembled in Congress must make.

The price of congressional inaction would be high. If federal bank regulators are permitted to transform their supervisory authority over the Nation's banks into a supervisory authority over the Nation's economic and commercial life, it will be a short step to regulatory tyranny, a regime where Americans are ruled not by laws but by men operating free from the bonds of law and from the need to answer at the ballot box.