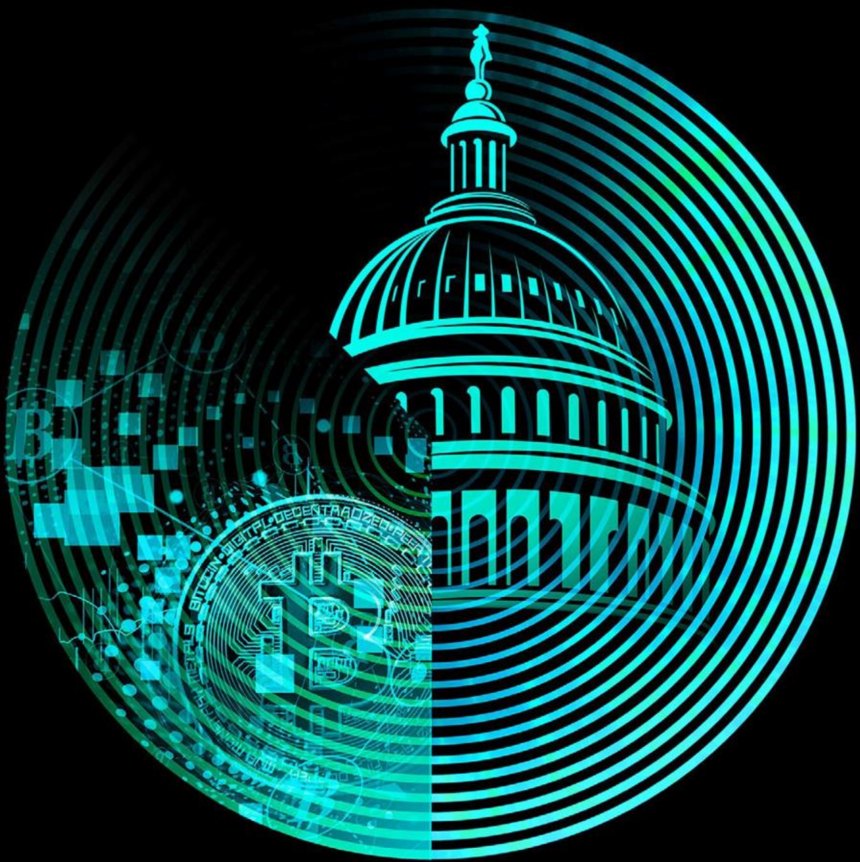
Deloitte.

CENTER for REGULATORY STRATEGY AMERICAS



Banking regulators reinforce wall for bank involvement in crypto-assets

On January 3, 2023, the Federal Reserve Board of Governors (FRB), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) together issued a *Joint Statement on Crypto-Asset Risks to Banking Organizations* that reinforces and sets a clear line in the sand, making it clear that while some crypto-asset banking activities are likely permissible, they are not advisable.[1] Their definition of crypto-assets is very broad, including stablecoins and other tokenized assets.

The Joint Statement follows four recent regulator industry letters from the agencies and the New York Department of Financial Services (NYDFS) identifying the risks and protocols for supervised firms planning to or already engaging in cryptocurrency activities.

As banking organizations continue to explore tokenized deposits, payment networks, crypto custody and other consumer facing transactions involving crypto-assets and stablecoins, the agencies have created notification and non objection processes to gauge the level of participation in and nature of these activities. The Joint Statement and four letters described here highlight the potential risks that banks should consider, give warning of the agencies' close attention to crypto-related events, and establish a clear and mandatory line of communication with supervisory staff.

Forceful language reinforces line in the sand

The banking agencies' language in the Joint Statement is the **most forceful to date**, as it clearly calls into question the safety and soundness practices of those engaging in crypto-assets, including banks with concentrated exposure to the crypto assets sector.

The Joint Statement's new wall for banking involvement in crypto-assets states:

> "Based on the agencies' current understanding and experience to date, the agencies believe that issuing or holding as principal crypto-assets that are issued, stored, or transferred on an open, public, and/or decentralized network, or similar system **is highly likely to be inconsistent with safe and sound banking practices. Further, the agencies have significant safety and soundness concerns** with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector."[2]

The statement notes that banks are "neither prohibited or discouraged from providing banking services to any customer", not specifically referring to crypto-assets. Later in the statement, regulators express clear discomfort with their experiences to date of banks engaging with crypto-assets and the crypto-asset sector. This likely foreshadows supervisory issues in the form of MRAs, MRIAs, other enforcement actions and generally very slow non-objection/approval processes.

The broad scope of crypto-assets covered by the statement ("any digital asset implemented using cryptographic techniques") provides a lens into the breadth of assets for which regulators are looking to apply their non-objection/approval processes.

The Financial Stability Oversight Council (FSOC) report gives further perspective into the intended scope

"The term crypto-assets encompasses many assets commonly referred to as "coins" or "tokens" by market participants. While other assets may involve digital representations of value, such assets are only crypto-assets if they rely on distributed ledger technology (DLT) or similar technology. For example, an equity security placed at a central securities depository may involve a digital representation of value, but ownership is determined through centralized records, not DLT."[3]

Risks noted by banking regulators

The Joint Statement highlights a number of key risks related to crypto-assets:

- "Risk of fraud and scams among crypto-asset sector participants.
- Legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings.
- Inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties.
- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.
- Susceptibility of stablecoins to run risk, creating potential deposit outflows for banking organizations that hold stablecoin reserves.
- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements. These interconnections may also present concentration risks for banking organizations with exposures to the crypto-asset sector.
- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.
- Heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance."[4]

Taken together, it is clear that the banking regulators are using their Joint Statement and notification processes to moderate and slow crypto-related activities at supervised firms. Each agency has issued guidance, broadly applicable to their respective supervised firms, requiring that at a minimum local agency staff be informed of crypto-related activities. NYDFS requires prior approval of any new or significantly different crypto- related activity and the OCC is requiring the agency's non-objection to notifications prior to commencing crypto-related activities.[5] The FRB and FDIC have taken similar approaches with the acceptance of both pre- and post-engagement notifications as well as plans to provide supervisory feedback in response to notifications.

In our view (and this was further reinforced by the Joint Statement and industry letters), banking regulators are treating new crypto/digital asset product offerings very much akin to new licensing/application efforts. Which means business plans, financials, governance, risk and compliance materials will need to be developed and reviewed prior to non-objection/permission.

Banking regulator crypto-related activity notification letters

Theme	NYDFS[6]	FRB[7]	FDIC[8]	OCC[9]
Publication date	December 15, 2022 (Industry Letter)	August 16, 2022 (Supervision and Regulation Letter)	April 7, 2022 (Financial Institution Letter)	November 18, 2021 (Interpretive Letter)
Institution scope	Applies to New York banking organizations, including branches and agencies of foreign banking organizations (FBOs).	Applies to all banking organizations supervised by the Federal Reserve.	Applies to FDIC-supervised institutions.	Applies to national banks and Federal savings associations.
Permissibility	The guidance does not interpret existing law or regulation and does not take a position on the types of activities that may be permissible.	The letter does not address the legal permissibility of any specific crypto-related activity. Rather, the letter places the onus on banking organizations to study the permissibility of crypto-related activities pursuant to laws such as the Federal Reserve Act, Bank Holding company Act, Home Owners' Loan Act, Federal Deposit Insurance Act, etc.	The letter does not address the permissibility of any specific crypto-related activity.	The activities legally permissible for a bank are clarified through prior Interpretative Letters 1170,[10] 1172,[11] and 1174[12] through the period of 2020 and early 2021, which includes cryptocurrency custody services, holding dollar deposit reserves backing stablecoin, distributed ledger and stablecoin activities.

Theme	NYDFS	FRB	FDIC	OCC
Communication considerations	Requires banks to seek prior approval **before commencing any new or significantly different crypto-related activity:** • Inform NYDFS a minimum of 90 days before commencing the activity • Work with NYDFS to confirm whether approval is required • Provide sufficient information regarding safety and soundness, including implications for customers	Suggests that applicable banking organizations **currently engaged or planning to engage** in crypto-related activities: • Notify the respective lead supervisory point of contact. • Stand up sufficient systems, risk management, and controls to promote the safe and sound execution of crypto-related activities.	Requires that applicable institutions **currently engaged in or planning to engage** in crypto-related activities: • Notify the FDIC (and state regulators). • Provide requested information to assess the underlying risks related to safety and soundness, consumer protection, and financial stability implications.	Requires the applicable banks to: • Provide written notification, to the supervisory office, of their **intention to engage** in crypto-related activities. • Demonstrate appropriate risk management and measurement process as well as sufficient controls are in place to conduct activity in a safe and sound manner.
Risk and materials considerations	• Business plan • Risk management • Corporate governance and oversight • Consumer protection • Financial • Legal and regulatory analysis	• Operational • Financial • Financial stability • Legal • Compliance • Consumer protection	• Credit • Liquidity • Market • Pricing • Operational • Systemic • Consumer protection	• Operational • Liquidity • Strategic • Compliance
Materials to submit	Institutions must provide at a minimum: • Written business plans describing relationship with strategic plans • Alignment of new activity to risk management framework and corporate governance framework • Consumer protection policies, procedures and disclosures • Pro-forma financials • Internal assessment of permissibility	A list of submission materials is not provided. However, banking organizations should be prepared to demonstrate the sufficiency of their systems, risk management, and controls.	The information requested by the FDIC will vary on a case-specific basis depending on the type of crypto-related activity.	A bank should demonstrate in its submission the risks associated with cryptocurrency activities understanding of its compliance obligations (e.g. Bank Secrecy Act, anti-money laundering, sanctions, Commodity Exchange Act, and consumer protection).
Notification response	Objection/ Non-Objection	Supervisory feedback	Supervisory feedback	Objection/ Non-Objection

Five insights from the NYDFS guidance you should know:[13]

1. Approval required: NYDFS is requiring departmental approval of all New York banking organizations, as well as branches and agencies of foreign banking organizations, seeking to commence new or significantly expanded crypto-related activity. **New or significant activity is defined** as activity that:
   a. May raise a legal or regulatory issue about the permissibility of the product, service, or change;
   b. May raise safety and soundness, including operational, concerns; or,
   c. May cause the product or service to be significantly different from that previously approved.
2. Applicability: The letter applies only to banks and does not apply to non-depository institutions with a "BitLicense" under New York's "Part 200" regulation (23 NYCRR Part 200). Prior departmental approval for activity does not give a bank authorization for new types of activity and does not apply to other institutions seeking to undertake the approved activity.
3. Approval process initiation: Banks should inform NYDFS at least 90 days before commencing a new or significantly different crypto activity. After the bank initiates the approval process, NYDFS and the bank will work together to confirm whether approval is required, identify the needed materials for approval, and establish a timeline.
4. Required information: As part of the approval process, NYDFS will require sufficient information on the proposed activity across a variety of areas affecting the institution's safety and soundness, implications for customers and other users of the product, including:

- Business plan: written business plans describing relationship with strategic plans.
- Risk management: alignment of new activity to risk management framework including crypto-specific risks (operational, credit, market, capital, liquidity, cyber security and fraud, third-party service providers, legal and compliance, reputational and strategic).
- Corporate governance: internal approvals of board and management and evidence of their understanding of risk, alignment of the activity to the risk appetite framework, and oversight including board committee delegation and oversight of the development of policies and procedures.
- Consumer protection: consumer protection policies, procedures and disclosures and interactions with third-parties
- Financials: explanation of expected impacts on the bank's capital and liquidity profile
- Legal and regulatory analysis: internal assessment of permissibility, key legal risks and mitigants

When compared against the what the three federal banking regulators require in their notification, NYDFS is much more prescriptive.

5. Checklist: As part of the guidance, NYDFS prepared a checklist of materials for banks to use as they prepare written submissions. The checklist includes suggested documents on operating models, technology architecture, controls, policies, and procedures.

Five actions to consider taking:

1. **Engage with regulators:** Engage early and often with regulators on the proposed business model and plans. Demonstrate a clear linkage between the bank's strategy and new proposed products. Confirm awareness, knowledge, and understanding of new products and associated risks across the board, senior management and business lines, independent risk and compliance functions, as well as internal audit.
2. **Tailor assessment to regulator's priorities:** Conduct a preliminary assessment to determine the legal applicability of activities pursuant to applicable banking law (and whether notification / non objection / approval is required), ensuring the core safety and soundness activities and policies are addressed (e.g., risk assessment, policy and procedure impacts, risk appetite impacts, new product approval). Provide sufficient detail and supporting information to establish comfort with regulators that potential risks associated with the proposed activities have been considered and to the extent possible, mitigated. Complete a risk assessment to quantify risks tied to specific products and activities.
3. **Prepared to be challenged:** Treating new products in an end-to-end fashion (e.g., developing a business plan, assessing impacts to risk appetite/risk and control processes) will go a long way to satisfying "application/licensing" like processes being stood up at the various banking regulators. Consider ways in which regulators may challenge the proposed activities and be prepared to address potential challenges and emerging risks. Be prepared to provide a walkthrough of the key concepts, risks, and business model to establish a common understanding of the nomenclature and verify that what is being proposed is understood. Factor the magnitude of risk associated with crypto-related activities into the organization's risk appetite and broader risk management practices.
4. **Anchor new products in strategy:** Confirm that the business model and proposed use cases have a purpose and create value for customers and the bank (e.g., why is this being pursued) and ultimately is anchored in the bank's strategy.
5. **Recognize comprehensive risk:** Understand involved counterparties and corresponding counterparty credit, potential systemic, third-party, and other risks. This may become increasingly challenging with a public blockchain given the opacity of the node validators, so forward-looking analysis of stress events (e.g., the failure or bankruptcy of key counterparties) will likely be informative.

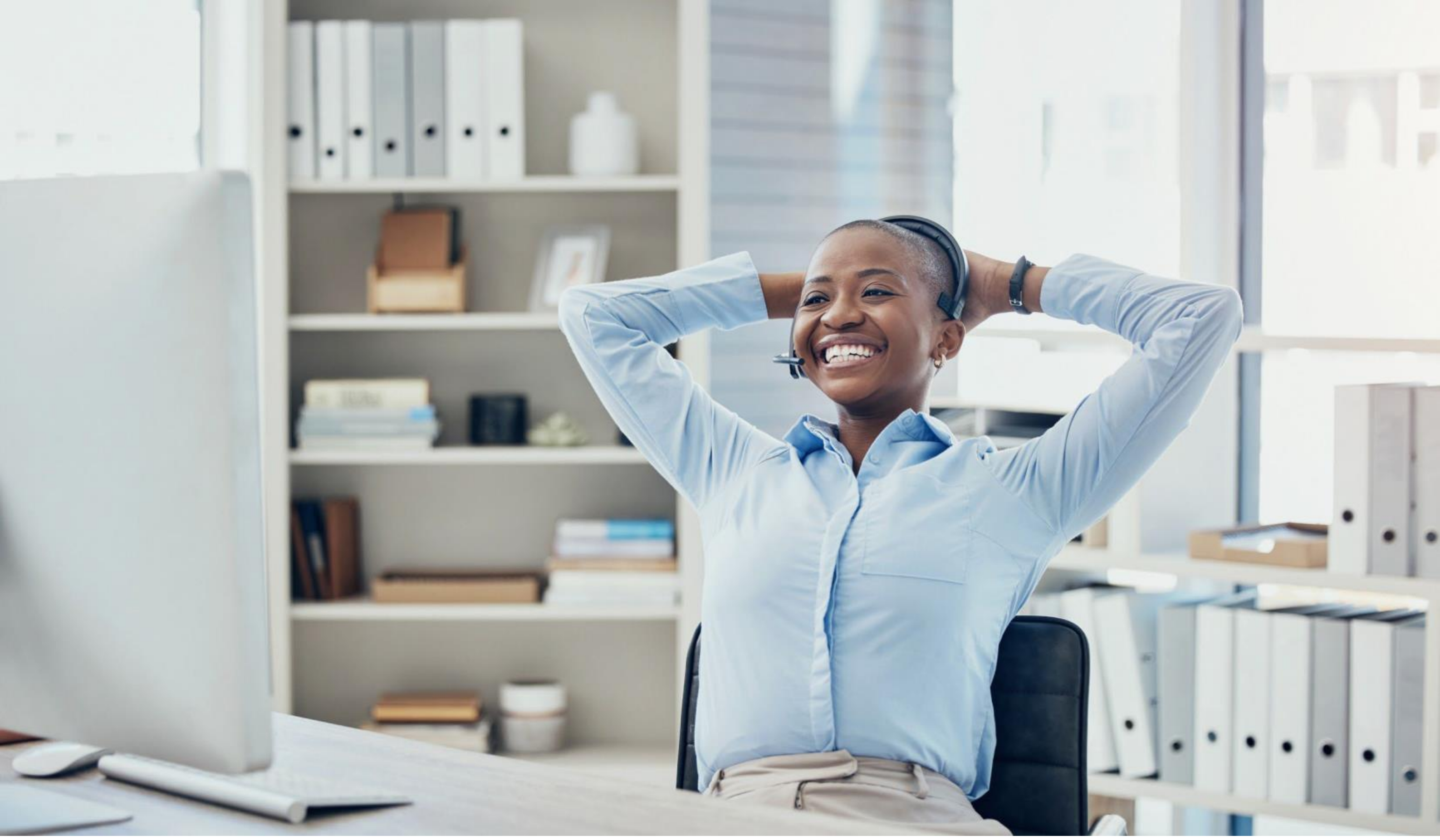
For additional perspective on recent developments

- Replay: Looking for the long view on US digital assets policy and regulation
- FDIC heightens its enforcement of the Federal Deposit Insurance (FDI) Act
- Bipartisan House bill proposes federal framework for payment stablecoins
- Digital assets policy primer: Fall 2022
- So, You Want to be a Crypto Bank?
- So, You Want to be a Stablecoin Issuer?

Endnotes

1. Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), "Joint Statement on Crypto-Asset Risks to Banking Organizations," join statement, January 3, 2023.
2. Ibid.
3. Financial Stability Oversight Council (FSOC), "Report on Digital Asset Financial Stability Risks and Regulation," October 3, 2022.
4. FRB, OCC, FDIC, "Joint Statement on Crypto-Asset Risks to Banking Organizations," join statement, January 3, 2023.
5. New York Department of Financial Services (NYDFS), "Prior Approval for Covered Institutions' Virtual Currency Related Activity," industry letter, December 15, 2022; and OCC, "OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities and Authority of OCC to Charter National Trust Banks," news release, November 23, 2021.
6. NYDFS, "Prior Approval for Covered Institutions' Virtual Currency Related Activity," industry letter, December 15, 2022.
7. FRB, "SR 22-6 / CA 22-6 Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking," supervision and regulation letter, August 16, 2022.
8. FDIC, "FDIC: FIL-16-2022: Notification of Engaging in Crypto-Related Activities," financial institution letter, April 7, 2022.
9. OCC, "OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities and Authority of OCC to Charter National Trust Banks | OCC," news release, November 23, 2021.
10. OCC, "Interpretive Letter 1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers," interpretive letter, July 22, 2020.
11. OCC, "Interpretive Letter 1172 OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves," interpretive letter, September 21, 2020.
12. OCC, "Interpretive Letter 1174, OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment," interpretive letter, January 4, 2021.
13. NYDFS, "Prior Approval for Covered Institutions' Virtual Currency Related Activity," industry letter, December 15, 2022.

.



Contacts

Richard Rosenthal
Principal | Deloitte & Touche LLP
rirosenthal@deloitte.com

Tim Davis
Principal| Deloitte & Touche LLP
timdavis@deloitte.com

Roy Ben-Hur
Managing Director | Deloitte & Touche LLP
rbenhur@deloitte.com

Kenneth Lamar
Senior Advisor to Deloitte & Touche LLP
kelamar@deloitte.com

Rich Mumford
Senior Advisor to Deloitte & Touche LLP
rmumford@deloitte.com

Deloitte Center for Regulatory Strategy

Irena Gecas-McCarthy
Principal | Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Michele Jones
Senior Manager | Deloitte Services LP
michelejones@deloitte.com

Kyle Cooke
Senior Regulatory Analyst | Deloitte Services LP
kycooke@deloitte.com

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2022 Deloitte Development LLC. All rights reserved.