FINTECH LAW REPORT
E-Banking, Payments & Commerce in the Mobile World

January/February 2025 ▪ Volume 28 ▪ Issue 1

FINTECHS BRANCHING INTO THE UNITED STATES

By Max Bonici and Stephen T. Gannon

Max Bonici is a partner in the Washington D.C. and New York offices of Davis Wright Tremaine LLP. Stephen Gannon is a partner in the firm's Richmond and Washington D.C. offices. Contact: maxbonici@dwt.com or stevegannon@dwt.com.

The federal banking agencies under a second Trump administration are expected to be more receptive to industry proposals geared toward growth. We've previously explored national trust banks[1] to streamline state licensing. Another option is for foreign banks to enter the U.S. market by establishing U.S. branches.

Because some countries have modernized their banking systems in ways that currently outpace the United States, certain non-U.S. fintechs may constitute foreign banks and be able to branch into the United States. This option allows them to do more activities more efficiently than U.S. fintechs are able to under the current U.S. framework.

KEY TAKEAWAYS

- Non-U.S. fintechs that engage in banking in home countries that the Federal Reserve has determined are subject to "Comprehensive Consolidated Supervision" ("CCS") can branch into the United States with the approval of the Federal Reserve and a state regulator or the Office of the Comptroller of the Currency ("OCC").
- Assuming a non-U.S. fintech obtains a federal branch license from the OCC, it can engage in practically every activity a national bank can, other than accepting FDIC-insured deposits. Many fintech lenders don't want to do that anyway. And it doesn't stop them from accepting uninsured deposits (*i.e.*, those above $250,000).
- Establishing a federal branch avoids the legal uncertainty involved with the OCC's "special purpose national bank charter" as well as 50-plus state money transmission, consumer lending, and

IN THIS ISSUE:

Thomson Reuters™

43251754

other licenses. It also avoids the chartering/acquisition and FDIC deposit insurance application process that can be subject to delays. One non-U.S. payments company[2] has already taken advantage of this option.

- U.S. fintechs cannot take advantage of this process or the legal clarity it provides. They are instead mired in an impasse between the states and the OCC about what national banks can do. The unequal treatment of non-U.S. versus U.S. fintechs is at odds with the principle national treatment for foreign banks.

FINTECHS AS "FOREIGN BANKS"

Under the International Banking Act of 1978 ("IBA") and the Federal Reserve's regulations, a foreign bank is any organization that is organized under the laws of a foreign country and that engages directly in banking activities usual in connection with the business of banking in the country where it is organized or operating (outside the United States).

The definition is broad and malleable enough to cover different kinds of financial institutions around the world. For instance, German and Japanese commercial banks, as well as groups of Canadian credit unions/cooperatives are considered foreign banks under this definition and have been able to branch into the United States.

Simply put—if the entity or organization is a foreign bank, it can seek to establish a U.S. branch.

CHOICE OF STATE OR OCC LICENSE, PLUS FEDERAL RESERVE APPROVAL

To establish a U.S. branch, a non-U.S. fintech (that is a foreign bank) may choose between a state license (for instance, New York or California) or a federal license from the OCC. The OCC will review:

- the financial and managerial resources and future prospects of the applicant foreign bank and the proposed federal branch;
- whether the foreign bank has provided the OCC with information to adequately assess the application and assurances that all information will be made available to the OCC on the operations and activities of the foreign bank and any of its affiliates the OCC deems necessary to enforce compliance with the IBA and other applicable federal banking statutes;

FinTech Law Report
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ● 6 Issues ● $ 1020.00

- whether the foreign bank and its U.S. affiliates are in compliance with applicable U.S. laws;
- the convenience and needs of the community to be served, including the record of the participating institutions' termination of individual customer accounts or categories of customer accounts or otherwise electing not to provide a person or category of persons with a financial service without assessing the risks posed by individual customers on a case-by-case basis;
- the effect of the proposed branch on competition in U.S. domestic and foreign commerce;
- whether the foreign bank is subject to CCS by its home country supervisor (or is working actively toward CCS);
- whether the foreign bank's home country supervisor approved or consented to the establishment of the federal branch; and
- whether adequate controls for the detection of money laundering are in place at the foreign bank.

Whichever license the non-U.S. fintech pursues, it must also obtain the approval of the Federal Reserve to establish a U.S. branch. The Federal Reserve will generally review for similar issues as the OCC, as well as:

- whether the home country is participating in multilateral efforts to combat money laundering;
- whether the appropriate supervisors in the home country may share information on the bank's operations with the Federal Reserve.

In the case that a foreign bank presents a risk to the U.S. financial stability, the Federal Reserve also may consider whether the home country of the foreign bank has adopted, or is making demonstrable progress toward adopting, an appropriate system of financial regulation for the financial system of the home country to mitigate this risk.

COMPREHENSIVE CONSOLIDATED SUPERVISION

Under the IBA, the Federal Reserve may only approve the establishment of a U.S. branch if it determines the foreign bank is subject to CCS, meaning the foreign bank is supervised or regulated such that its home country supervisor receives sufficient information on the worldwide operations of the foreign bank (including the relationships of the bank to any affiliate) to assess the foreign bank's overall financial condition and compliance with laws and regulations.

The Federal Reserve typically considers (among other things) the extent to which the home country supervisor:

- ensures that the foreign bank has adequate procedures for monitoring and controlling its activities worldwide;
- obtains information on the condition of the bank and its subsidiaries and offices through regular examination reports, audit reports, or otherwise;
- obtains information on the dealings and relationships between the bank and its affiliates, both foreign and domestic;
- receives from the bank financial reports that are consolidated on a worldwide basis, or comparable information that permits analysis of the bank's financial condition on a worldwide consolidated basis; and

- evaluates prudential standards, such as capital adequacy and risk asset exposure, on a worldwide basis.

Practically speaking, non-U.S. fintechs from countries that have previously received CCS determinations have the best chances of branching into the United States.

Summary of CCS Determinations and Active Branches/Agencies by Country

Americas	Europe*	Middle East & Africa	Asia-Pacific
Argentina	Austria	Bahrain	Australia
Brazil	Belgium	Egypt	China
Canada	Finland	Israel	Hong Kong
Chile	France	Kuwait	India
Colombia	Germany	Nigeria	Japan
Mexico	Greece	Saudi Arabia	Korea
Panama	Ireland	Turkey	Micronesia
Peru	Italy	United Arab Emirates	Singapore
Puerto Rico	Norway		Philippines
Uruguay	Portugal		Taiwan
	Spain		Thailand
	Sweden		
	Switzerland		
	Netherlands		
	United Kingdom		

**In certain cases, includes supervision under the Single Supervisory Mechanism.*

The Fed maintains a list[3] of the banks, branches, and other U.S. offices of non-U.S. banks.

BRANCHING INTO THE UNITED STATES

Establishing a U.S. branch is a substantial undertaking like chartering or acquiring a U.S. bank. A foreign bank that establishes a U.S. branch will generally—but with some notable exceptions—be treated as a bank holding company that is subject to Federal Reserve restrictions and requirements, even if the foreign bank does not own or control a U.S. bank. In addition, the U.S. branch and the foreign bank's U.S. operations will be subject to U.S. supervision and regulation.

And while U.S. branches are not subject to separate capital requirements—unlike a U.S. bank—federal branches must maintain a capital equivalency deposit ("CED"). Subject to certain requirements and approvals, a federal branch must establish and maintain a CED account with an eligible U.S. bank in an amount equal to at least 5% of the total liabilities of the federal branch. The OCC may require a higher amount.

These costs come with notable benefits. A federal branch can practically do everything a national bank can do, other than accept insured deposits.

	National Bank	Federal Branch
Accept insured deposits (≤ $250K)	■	
Accept uninsured deposits (> $250K)	■	■
Lend to consumers*	■	■
Lend to businesses	■	■
Directly access U.S. payments system	■	■
Fiduciary powers (with OCC approval)	■	■
Enjoy National Bank Act preemption of state laws	■	■
Trading and investment activities	■	■

**Federal branches do not ordinarily lend to consumers, but they are not expressly prohibited from doing so.*

NATIONAL TREATMENT CONSIDERATIONS

Since at least the enactment of the IBA in 1978, U.S. banking policy has sought to uphold the principle of national treatment. Under this principle, non-U.S. banks should largely be able to participate in the U.S. market to the same extent that U.S. banks can. Today, some non-U.S. fintechs arguably are *more favored* than U.S. fintechs because U.S. fintechs do not have any options akin to establishing a U.S. branch of a foreign bank. That's a big advantage for non-U.S. fintechs, particularly for those from countries for which the Fed has previously made a CCS determination.

We also note that some foreign banks are ahead of the U.S. in adopting digital asset tools and technologies. That could mean that once the U.S. regulatory hostility to digital assets dampens—which could likely happen in a second Trump administration[4]—foreign banks and their U.S. branches may be better positioned (at least for a time) to penetrate the U.S. markets in digital assets and blockchain because they are already using them in their home countries.

Congress and the OCC should work to rectify this disparity. In the meantime—and particularly under a new administration in 2025—non-U.S. fintechs might consider expansion into the United States via branching as an alternative to owning or controlling a U.S. bank or obtaining 50-plus state licenses as a non-bank lender, money transmitter, or other financial services provider.

ENDNOTES:

[1] https://www.dwt.com/blogs/financial-services-law-advisor/2024/11/why-fintechs-should-consider-national-trust-banks.

[2] https://www.dwt.com/-/media/files/blogs/financial-services-law-advisor/2025/ca1246.pdf?rev=c7c561c40e6d404683b0c6600a791a63&hash=AA23EE7BEFC087D1A61598FFE5510346.

[3] https://www.federalreserve.gov/releases/iba/.

[4] https://www.dwt.com/blogs/financial-services-law-advisor/2024/11/what-trump-could-do-with-crypto-and-digital-assets.

ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES: A BREAKDOWN OF THE TREASURY REPORT FOR FINTECH FIRMS

By Matthew G. White and Alexander F. Koskey

Matthew White is co-chair of the Financial Services Cybersecurity and Data Privacy Team at Baker Donelson, based in the firm's Memphis office. Alexander Koskey is co-chair of the Financial Services Cybersecurity and Data Privacy Team, based in Baker Donelson's Atlanta office. Contact: mwhite@bakerdonelson.com or akoskey@bakerdonelson.com.

Artificial intelligence ("AI") has been *the* buzzword of the last two years, and now it's Treasury's turn to chime in. In December 2024, the U.S. Department of the Treasury released its much-anticipated Report[1] entitled "Uses, Opportunities, and Risks of Artificial Intelligence in Financial Services." Spoiler alert: it's a comprehensive deep dive into how AI is reshaping financial services and the regulatory landscape. For FinTech firms, the stakes just got higher. Let's unpack the Report's highlights and figure out what's in it for you—besides sleepless nights and more compliance headaches.

THE BIG PICTURE: AI'S ROLE IN FINANCIAL SERVICES

The Treasury's Report highlights AI's transfor-

mative potential in financial services, underscoring its role in everything from fraud detection to personalized customer service. Key opportunities identified in the Report include:

- *Operational Efficiency*: AI can potentially streamline back-office operations, optimize trading algorithms, and automate compliance tasks.
- *Enhanced Customer Experiences*: From chatbots to tailored financial advice, AI enables hyper-personalization, potentially boosting customer satisfaction and loyalty.
- *Risk Management*: Advanced analytics powered by AI can better predict and mitigate risks, helping firms stay one step ahead of emerging threats.

However, with great power comes great responsibility—and, of course, regulatory scrutiny. The Treasury doesn't mince words about the risks, including: bias in AI models, cybersecurity vulnerabilities, systemic risks due to over-reliance on a few large AI providers, and the potential for misuse of AI in fraudulent schemes.

WHY THIS MATTERS TO FINTECH FIRMS

FinTech companies are frequently at the forefront of integrating AI into financial services offerings, but they also operate under a microscope. The Treasury's Report sends a clear message: regulators are watching closely, and the bar for compliance is rising. Key areas FinTech firms should focus on include:

- *Regulatory Scrutiny*: FinTech firms must not only align their AI practices with new laws, but also with existing laws, including fair lending, anti-money laundering ("AML"), and privacy regulations. The Report suggests that regulators are exploring how to adapt existing frameworks to account for AI's nuances.
- *Ethical AI Use*: Bias in AI models can result in discriminatory practices, particularly in lending and credit decisions. FinTech firms must proactively address these risks to avoid reputational damage and regulatory penalties.
- *Cybersecurity and Resilience*: AI-powered tools are a double-edged sword. While they can enhance cybersecurity, they also introduce new attack vectors. The Report emphasizes the importance of robust defenses against AI-driven cyber threats.
- *Systemic Risks*: Over-reliance on a handful of AI providers could create systemic vulnerabilities. FinTech firms need to diversify their AI ecosystems and develop contingency plans.

KEY TAKEAWAYS AND ACTION ITEMS FOR FINTECH FIRMS

So, what does this all mean for FinTech firms? Here's your playbook for navigating the Treasury's AI Report:

1. Audit Your AI Models:

- Perform regular audits to identify and mitigate any bias in your AI algorithms.
- Use diverse datasets and transparent methodologies to ensure fairness.
- Document your decision-making processes to demonstrate compliance.

2. Enhance Cybersecurity Measures:

- Implement AI-driven tools to detect and respond to cyber threats.
- Conduct regular penetration testing and vulnerability assessments.
- Train your staff to recognize and respond to AI-driven phishing attacks.
- Practice your incident response plan through tabletop exercises.

3. Prioritize Ethical AI Practices:

- Establish an ethics committee or appoint an AI ethics officer.
- Develop and enforce policies for the ethical and appropriate uses of AI.
- Engage third-party experts and/or frameworks to validate your AI practices.

4. Diversify Your AI Ecosystem:

- Avoid vendor lock-in by using multiple AI providers.
- Consider investing in in-house AI capabilities to reduce dependency on third-party tools.
- Collaborate with industry peers to share insights and best practices.

5. Prepare for Increased Regulation:

- Stay informed about evolving AI regulations and guidance.
- Engage with regulators proactively to shape the conversation.
- Participate in industry associations to advocate for practical regulatory frameworks.

SURVIVING THE AI REVOLUTION

If the Treasury's Report has you reaching for a stress ball, you're not alone. Navigating the complex world of AI in financial services can feel like trying to read the terms and conditions of a software update—overwhelming and vaguely threatening. But remember, compliance isn't just about avoiding fines; it's about building trust with your customers and partners. And if all else fails, there's always coffee—lots and lots of coffee.

CONCLUSION: THE ROAD AHEAD

The Treasury's Report may serve as a wake-up call for FinTech firms. AI offers unprecedented opportunities to innovate and grow, but it also comes with significant risks. By embracing ethical practices, strengthening cybersecurity, and staying ahead of regulatory changes, FinTech firms can harness AI's potential while minimizing its pitfalls.

In the end, the key to thriving in this AI-driven era is adaptability. As the Treasury Report reminds us, the future of financial services will be shaped by those who can balance innovation with responsibility. So, roll up your sleeves, FinTech pioneers: the AI revolution waits for no one.

ENDNOTES:

[1] https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf.

DAOS WATCH OUT: FEDERAL COURT IN CALIFORNIA DECIDES A DAO CAN BE A GENERAL PARTNERSHIP

By Carl Fornaris, Andrew Maxwell Hinkes, Kimberly A. Prior and Daniel T. Stabile

Carl Fornaris, Andrew Hinkes, Kimberly Prior and Daniel Stabile are partners in the Miami office of Winston & Strawn LLP. Law Clerk Duoye Xu also contributed to this article. Contact: cfornaris@winston.com or ahinkes@winston.com or kprior@winston.com or dstabile@winston.com.

On November 18, 2024, in *Samuels v. Lido DAO*,[1] the United States District Court for the Northern District of California denied some defendants' motions to dismiss, finding that the plaintiff sufficiently alleged that a decentralized autonomous organization ("DAO")[2] is a partnership under California law, and consequently that these defendants may be liable as general partners. The court relied chiefly on the plaintiff's argument that these defendants "meaningfully participated"[3] in the DAO's governance.

BACKGROUND

A DAO is an organization that utilizes blockchain[4]-based technology tools, including smart contracts, to make decisions and to control property. A DAO usually allows its participants to act by way of "governance tokens" that empower their holders to participate in the governance of the DAO, including voting on decisions that may affect certain property.[5] Since the launch of the first major DAO in 2016 (aptly named "The DAO"), thousands of DAOs have been formed. DAOs vary in purpose and scope; some are formed to engage in projects, to manage software, to invest, to provide services, or for charitable purposes.

The *Samuels v. Lido DAO* case concerns the Lido DAO, a DAO formed to govern aspects of the Lido liquid staking protocol,[6] and certain purchasers of the LDO token. The plaintiff purchased LDO tokens via a digital asset exchange and alleged that he sustained a loss when he later sold those tokens. The plaintiff sued Lido DAO and four holders of a significant amount of LDO tokens. He claimed that Lido DAO, as a partnership, violated federal securities law,[7] and the four significant token holders, alleged to be general partners of that partnership, should be liable for the DAO's violations. The defendants moved for dismissal arguing, among other things, that the DAO is not capable of being sued because it is not a legal entity and that it is not a partnership because, among other things, it observes no formalities normally associated with a partnership.

According to the plaintiff and the Court's judicial notice, Lido DAO is in the business of managing aspects of the Lido Protocol and it maintains certain service fees it collects.[8] It was founded by three individuals whose whereabouts are either unknown or outside the United States. Some legal entities were incorporated to facilitate its creation, but these entities "vigorously repeat in their legal documentation" that they do not control Lido DAO.[9] After Lido DAO was founded, its LDO tokens were sold and later became listed on several major exchanges. Some of its 70-plus employees, including a business development lead and a chief marketing officer, worked on or promoted the listings.[10]

THE COURT'S REASONING

The Court rejected the argument that Lido DAO is merely software that cannot be sued. This argument was advanced by a limited liability company

("LLC") created by a subset of LDO token holders that itself was not sued by the plaintiff, but was formed to make a limited appearance in the lawsuit "to prevent entry of default judgment against Lido."[11] Although the LLC's standing to participate in the lawsuit was questioned by the Court,[12] the plaintiff did not object to the LLC's appearance and the Court considered the LLC's arguments.[13] The Court also noted that the DAO is "a type of organization that seems designed, at least in part, to avoid legal liability for its activities" without elaborating on the reason for such characterization.[14]

The Court accepted the plaintiff's allegations that "Lido DAO is jointly operated by 'large' holders of LDO voting those tokens to cause the DAO to make business decisions," and "Lido DAO's partners are those that have the capacity to meaningfully participate in Lido DAO's business."[15]

Defendants argued that Lido DAO could not be a partnership under California law because California law requires all partners to consent to join a partnership and repurchase of interests by the partnership when a partner leaves a partnership, and because LDO tokens can be freely bought and sold in the open market. However, the Court found that these provisions are only default rules and, based on the facts alleged by the plaintiff, one can reasonably infer that the founding partners of the Lido DAO had opted out of these default rules.[16]

The Court noted that, at the pleadings stage, the plaintiff does not need to identify all general partners of the alleged partnership. The Court also noted that explicit agreement to share profit and loss is not necessary to find the existence of a partnership under California law. In addition, the Court decided that the entities established to facilitate the creation of Lido DAO are not an "affirmative choice of another corporate form [that] weighs against the existence of a partnership," because they do not control Lido DAO; the corporate forms of the holder defendants are also irrelevant, because "California law expressly provides that corporations and other corporate entities can be members of general partnerships."[17]

The Court found that the plaintiff has sufficiently alleged that three of the four large LDO holder defendants meaningfully participated in the Lido DAO partnership:

- One holder defendant was alleged to have "helped 'influence[]' and 'guide[]' the development of Lido and the DAO's website heralded [the defendant's] ability to 'lend its expertise to Lido DAO [sic] governance.' "[18]
- Another holder defendant was alleged to have "announced itself that it would contribute to Lido DAO as a 'governance participant,' and in at least one instance did express a view on DAO governance"; the plaintiff also alleged that this holder defendant purchased tokens worth US$70M.[19]
- A third holder defendant presents "a closer call." The plaintiff alleged that "[a]fter an initial purchase of US$25M worth of LDO, [the defendant] purchased even more tokens, noting that it was 'looking forward to being more active in governance' and that it was 'uniquely positioned to lend its expertise to Lido DAO [sic] governance.' And it was able to purchase these tokens because it voted for them to be sold to it."[20]

However, the Court dismissed one defendant, finding that the plaintiff failed to allege specific facts:

- "[The complaint noted] only that one of [the defendant's] partners praised Lido DAO, that [the defendant] was chosen to get involved

> with the DAO because it could add its 'expertise in the successful development of distributed protocols' to the DAO, and that it participated in a sale in which it, along with other entities, purchased 30 million LDO. It [did] not allege that [the defendant] participated in Lido DAO governance or made any statements about doing so."[21]

IMPLICATIONS

Other courts have previously held that a DAO can be a general partnership or unincorporated association. In *CFTC v. Ooki DAO*, also decided in the Northern District of California, the Court held that a DAO can be an unincorporated association that can be served—through its chat box and online forum—and can be liable under the Commodity Exchange Act.[22] In a 2023 decision in *Sarcuni v. bZx DAO*, the United States District Court for the Southern District of California held that all token holders of a DAO can be partners in a partnership.[23] This view, however, is not unanimously held.[24]

There are still many uncertainties surrounding the nature of DAOs and the status of participants in those DAOs. While the *Samuels* Court's reasoning was mostly based on the scope of the partnership alleged by the plaintiff, which includes only those large holders with "the capacity to meaningfully participate in Lido DAO's business,"[25] the Court left open the possibility of a broader group, including all DAO token holders or everyone who has voted on a proposal in the DAO, or a narrower group, including only the founders of the DAO.[26] If this "meaningful participation" approach is applied, courts will grapple with complex legal and factual questions to establish which token holders are meaningfully participating in the DAO's affairs. Similarly, the Court's decision relied on California law to determine whether the plaintiff sufficiently alleged the existence of a general partnership; it is possible that Courts in other states may reach different conclusions based upon differing state laws. That may result in a single DAO having different legal status across different states.

The Court's general characterization of the DAO being an organization type used to avoid legal liability is also alarming to the digital assets industry sector. While the Court did not elaborate on the specific reason for such characterization, the founders, participants, and promoters of DAOs may need to more clearly demonstrate the legitimate business and social benefits of DAOs—such as facilitating decentralized collaboration—when interacting with courts, regulators, and the public.

Holders of DAO tokens should consider the potential exposure to partnership liability and be especially careful when purchasing DAO tokens in large quantities, participating in the governance of a DAO, or making representations about participation in a DAO. Deployers of DAOs may elect to "wrap" their DAO by forming a legal entity to conduct some or all the DAO's activities. Many DAOs elect to "wrap" themselves by delegating some actions to an ownerless Cayman "foundation company" that is limited by shares, and that employs professional directors who are entrusted with keys to DAO treasuries and are empowered to engage in legally significant activities where certainty as to legal status is required, such as hiring vendors and signing legal agreements. A DAO may also be formed as a legal entity. Some states have created bespoke legal entity types expressly for DAOs.[27] Wyoming recently approved a new type of entity known as the "decentralized unincorporated non-profit association" ("DUNA"), which makes the DAO itself a legal entity, provides liability protection for DAO token holders, and clarifies tax treatment for any value that flows to token holders

from the DAO.[28] As entrepreneurs continue to experiment with the use of digital assets, new technologies built with blockchains and smart contracts, and to innovate in their governance approaches, we expect to see states continue to experiment with new approaches to protecting those who interact with DAOs.

ENDNOTES:

[1]*Samuels v. Lido DAO*, Order re Motion to Dismiss, No. 23-cv-06492 (N.D. Cal. Nov. 18, 2024).

[2]What Is a Decentralized Autonomous Organization (DAO)?, Winston & Strawn, https://www.winston.com/en/legal-glossary/what-is-a-decentralized-autonomous-organization-dao.

[3]*Samuels v. Lido DAO*, Order re Motion to Dismiss, slip op. at 15.

[4]What Is Blockchain?, Winston & Strawn, https://www.winston.com/en/legal-glossary/blockchain.

[5]For more information, *see* our blog article, DAOs: Understanding the Basics, Winston & Strawn, https://www.winston.com/en/blogs-and-podcasts/the-playbook/daos-understanding-the-basics.

[6]*See* Lido DAO, https://docs.lido.fi/lido-dao/.

[7]The plaintiff alleged that because Lido DAO sold unregistered securities, he is entitled to recission under Section 12(a)(1) of the Securities Act of 1933. The Court rejected the defendants' argument that the plaintiff is not eligible under Section 12(a)(1) because he bought the tokens on the secondary market instead of buying directly from Lido DAO. The Court stated, among other things, "[L]iability for losses incurred from the purchase of unregistered securities only attaches to someone who 'offers or sells' those securities" (quoting Section 12(a)(1)), but the "offers or sells" requirement can be satisfied by successful solicitation motivated in part by the solicitor's or the security owner's financial interest. *Id.* slip op. at 2, 19. The Court found that the plaintiff has properly alleged solicitation, and such solicitation can be motivated by Lido DAO's financial interest because increased secondary market liquidity of LDO benefits Lido DAO. *Id.* slip op. at 20-21. The court also held that liability under Section 12(a)(1) is not limited to public offerings. *Id.* slip op. at 2, 23-27.

[8]*Samuels v. Lido DAO*, Order re Motion to Dismiss, slip op. at 3-4.

[9]*Id.* slip op. at 3.

[10]*Id.* slip op. at 4-7.

[11]*Id.* slip op. at 7; *Samuels v. Lido DAO*, Dolphin CL, LLC's Motion to Dismiss Plaintiff Andrew Samuels's Amended Complaint as to "Lido DAO," at 1 n.2 (N.D. Cal. July 11, 2024).

[12]*Samuels v. Lido DAO,* Order re Motion to Dismiss, slip op. at 7-9.

[13]*Id.* slip op. at 8. According to the court, the plaintiff was suing the "entity that operates the particular Lido deployment" and he has alleged that Lido DAO engaged in "the actions of an entity run by people," including "mak[ing] decisions through tokenholder votes, maintain[ing] a treasury where it keeps its retained percentage of staking rewards, and ha[ving] hired over 70 employees." (internal quotation marks omitted).

[14]*Id.* slip op. at 1.

[15]*Id.* slip op. at 10 (internal quotation mark omitted).

[16]*Id.* slip op. at 12-13.

[17]*Id.* slip op. at 13-14.

[18]*Id.* slip op. at 15 (internal citation omitted).

[19]*Id.* (internal citation omitted).

[20]*Id.* (internal citation omitted).

[21]*Id.* slip op. at 15-16 (internal citation omitted).

[22]*CFTC v. Ooki DAO*, Order Concluding That Service Has Been Achieved, No. 3:22-cv-05416 (N.D. Cal. Dec. 20, 2022) (Before this Order, the court ordered the CFTC to serve the founders of Ooki DAO who were also token holders, and the CFTC complied, but the court ultimately concluded that service to the founder-holders was not required by law.); *CFTC v. Ooki DAO*, No. 3:22-cv-05416 (N.D. Cal. June 8, 2023) (default judgment).

[23]*Sarcuni v. bZx DAO*, 664 F. Supp. 3d 1100, 1117-18, 15 Fed. R. Serv. 3d 935 (S.D. Cal. 2023).

[24]*See* SEC, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of

1934: The DAO (Release No. 81207, July 25, 2017), https://www.sec.gov/files/litigation/investreport/34-81207.pdf (discussing how token holders in The DAO were dispersed and pseudonymous, which "made it difficult for them to join together to effect change or to exercise meaningful control," with "thousands of individuals and/or entities that traded DAO Tokens in the secondary market—an arrangement that bears little resemblance to that of a genuine general partnership.")

[25]*Samuels v. Lido DAO*, Order re Motion to Dismiss, slip op. at 10.

[26]*See id.* slip op. at 11.

[27]*See* Wyoming Decentralized Autonomous Organization Supplement, Wyo. Stat. Ann. §§ 17-31-101-17-31-116 (2021); Vermont's Blockchain-Based Limited Liability Companies, Vt. Stat. Ann. tit. 11, §§ 4171-4176 (2018); Utah's Decentralized Autonomous Organization Act, Utah Code Ann. §§ 48-5-101-48-5-406 (2024); New Hampshire Decentralized Autonomous Organization Act, N.H. Rev. Stat. Ann. §§ 301-B:1-301-B:31 (effective July 1, 2025); Tennessee's Decentralized Organization, Tenn. Code Ann. §§ 48-250-101-48-250-115 (2022).

[28]*See* Wyoming Decentralized Unincorporated Nonprofit Association Act, Wyo. Stat. Ann. §§ 17-32-101-17-32-129 (2024).

CRYPTO WATCH: SEC ANNOUNCES CRYPTO TASK FORCE; SEC/COINBASE BATTLE ENTERS NEW PHASE; TORNADO GETS WINS; SEC DELAYS ETF DECISION; GENSLER BOWS OUT DEFIANT ON CRYPTO

SEC ANNOUNCES CRYPTO TASK FORCE

On January 21, 2025, Securities and Exchange Commission Acting Chairman Mark Uyeda announced the formation what he termed a "crypto task force" that would be charged with developing "a comprehensive and clear regulatory framework for crypto assets."[1]

Commissioner Hester Peirce, long considered the SEC Commissioner with the most positive attitude towards the cryptocurrency sector, will lead the task force. Richard Gabbert, Senior Advisor to the Acting Chairman, and Taylor Asher, Senior Policy Advisor to the Acting Chairman, were named the task force's Chief of Staff and Chief Policy Advisor, respectively.

The stated intention of the task force will be to collaborate with SEC staff and take public comments in order to "set the SEC on a sensible regulatory path that respects the bounds of the law." Uyeda, in a public statement, claimed that the task force marks a change in philosophy for the SEC, which heretofore has relied primarily on enforcement actions to regulate crypto.

This, in his reckoning, has meant that the Commission has proceeded "retroactively and reactively, often adopting novel and untested legal interpretations along the way. Clarity regarding who must register, and practical solutions for those seeking to register, have been elusive. The result has been confusion about what is legal, which creates an environment hostile to innovation and conducive to fraud. The SEC can do better."

The task force will be charged with helping "the Commission draw clear regulatory lines, provide realistic paths to registration, craft sensible disclosure frameworks, and deploy enforcement resources judiciously," the SEC said. In short, the task force will, as per Uyeda, "lead regulatory policy on crypto."

The SEC said the task force will "operate within the statutory framework provided by Congress and

will coordinate the provision of technical assistance to Congress as it makes changes to that framework . . . coordinate with federal departments and agencies, including the Commodity Futures Trading Commission, and state and international counterparts."

In a statement, Peirce said "this undertaking will take time, patience, and much hard work. It will succeed only if the Task Force has input from a wide range of investors, industry participants, academics, and other interested parties."

SEC/COINBASE BATTLE ENTERS NEW PHASE

In January, the SEC's battle with Coinbase Global Inc. encountered new twists in various courtrooms. First, the Third U.S. Circuit Court of Appeals issued a ruling, 3-0, which mandated that the SEC must offer a more precise explanation of why it turned down a request from Coinbase to develop a set of regulations to cover cryptocurrency assets. The Court did not, however, reverse the SEC's July 2022 decision to deny Coinbase's request.

Coinbase has argued in court that the SEC has been applying existing, and inadequate, securities laws to digital assets, thus prompting a need for new rules. As per the Court ruling, "Coinbase argued in its petition that the existing securities-law framework does not account for certain unique attributes of digital assets, which make compliance economically and even technically infeasible. It also asserted that the SEC has exacerbated these difficulties by failing to articulate a clear and consistent position about when a digital asset is a security, and thus subject to the federal securities laws at all."[2] A June 2023 SEC enforcement action is pending against Coinbase, alleging that the latter's trading platform for digital assets operates as an unregistered broker, exchange and clearing agency.

The SEC has said its crypto regulations may change based on "numerous undertakings" and that developing new rules would take it away from other duties. "A single sentence disagreeing with the main concerns of a rulemaking petition is conclusory and does not provide us with any assurance that the SEC considered Coinbase's workability objections, nor does it explain how it accounted for them," wrote Judge Thomas L. Ambro.

Ambro wrote that the SEC has taken a general position that some digital assets may qualify as securities and has indicated it could directly address the issues raised by Coinbase through some future rulemaking process. "It has said that it believes the existing securities-law framework is not unworkable for digital assets, but we have no basis in the record for determining why it believes that or how it arrived at that conclusion," Ambro wrote. "This explanation is not 'slim'—it is 'vacuous.' " The Court said the SEC must provide a more complete explanation for its "insufficiently reasoned" decision.

"The SEC repeatedly sues crypto companies for not complying with the law, yet it will not tell them how to comply," Judge Stephanos Bibas wrote in a concurrence. "That caginess creates a serious constitutional problem; due process guarantees fair notice."[3]

And Coinbase further benefited when a judge granted its request to chase a narrow appeal of the SEC's accusations about Coinbase trading crypto securities. Coinbase is allowed to lobby the U.S. Court of Appeals for the Second Circuit to find that the SEC's accusations against Coinbase—that the latter improperly handled the trading of unregistered securities—are unfounded.

On January 7, Judge Katherine Polk Failla of the U.S. District Court for the Southern District of New York agreed to approve a request from Coinbase to ask the higher court to consider one core question in the dispute, in a process known as an interlocutory appeal.

While noting that "the Court does not appreciate, and will not co-sign, Coinbase's efforts to cast aspersions on the SEC's approach to crypto-assets, the fact remains that [there are] conflicting decisions on an important legal issue necessitate the Second Circuit's guidance,"[4] Failla wrote.

Central to the SEC/Coinbase battle is whether certain tokens traded on the platform should be considered securities. Coinbase has argued that crypto token issuers who trade in its secondary markets don't technically owe anything to token buyers, and thus the tokens do not meet the legal standard for a security, the so-called *Howey* test.

Failla said she granted Coinbase's request "because it presents a controlling question of law regarding the reach and application of *Howey* to crypto-assets, about which there is substantial ground for difference of opinion, and the resolution of which would advance the ultimate termination of the SEC's enforcement action."

With SEC leadership changing hands to Republican control and the announcement of a crypto task force (see above), there's now substantial potential that the SEC will be developing crypto regulations in short to medium term future, market observers said.

TORNADO CASH GETS WINS

On January 22, the Fifth Circuit Court of Appeals ordered the U.S. Treasury's Office of Foreign Assets Control ("OFAC") to remove addresses linked to Tornado Cash from a list of Specially Designated National and Blocked Persons ("SDN").

Tornado's crypto mixing service had been banned by OFAC in August 2022, following its alleged use by hackers, including North Korea's Lazarus Group, to launder stolen crypto. OFAC had placed Tornado Cash on the SDN List, which prohibits dealings with "all real, personal, and other property and interests in property" that Tornado Cash may have, including, under OFAC's interpretation, any underlying smart contracts

Last November the Fifth Circuit Cort of Appeals had sided, 3-0, with users of Tornado Cash software—a crypto mixer that anonymizes crypto asset transactions—by holding in *Van Loon v. Department of the Treasury* that the company's immutable smart contracts are not "property" for purposes of sanctions under the International Emergency Economic Powers Act ("IEEPA").[5]

Six Tornado Cash users had sued, arguing that Tornado Cash smart contracts do not fall under OFAC supervision because such immutable smart contracts are not defined as "property" under the IEEPA.

While a district court held that these smart contracts were indeed "property," and that Tornado Cash was an entity capable of being designated under the IEEPA, the Fifth Circuit reversed and remanded the case to the lower court. While noting OFAC's money-laundering concerns, the court noted that the plain meaning of the term "property" requires something "capable of being owned." The court described the smart contracts at issue as being only "software code" deployed by individuals without contractual counterparties and further held that these contracts are not controlled by anyone and thus should not be considered "property" under the IEEPA.[6]

SEC DELAYS ETF DECISION

The SEC said it would need two additional months to decide whether an exchange-traded fund ("ETF") that has been designed as an all-purpose cryptocurrency portfolio can be listed on the New York Stock Exchange's electronic securities exchange, as per a January 14 regulatory filing.[7]

The filing came in response to the NYSE's December request for permission to list the Bitwise 10 Crypto Index Fund on NYSE Arca. Bitwise's proposed ETF would be the first diversified spot crypto ETF in the U.S. market and the first U.S. ETF to hold alternative cryptocurrencies, or "altcoins."

In its filing, the SEC said that on November 14, 2024, NYSE Arca Inc. filed "a proposed rule change to list and trade shares of the Bitwise 10 Crypto Index Fund under Proposed NYSE Arca Rule 8.800-E (Commodity and/or Digital Asset-Based Investment Interests). The proposed rule change was published for comment in the Federal Register on December 3, 2024. The Commission has received no comments on the proposal."

"Section 19(b)(2) of the Act provides that within 45 days of the publication of notice of the filing of a proposed rule change, or within such longer period up to 90 days as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or as to which the self-regulatory organization consents, the Commission shall either approve the proposed rule change, disapprove the proposed rule change, or institute proceedings to determine whether the proposed rule change should be disapproved. The 45th day after publication of the notice for this proposed rule change is January 17, 2025."

[But] "the Commission finds it appropriate to designate a longer period within which to take action on the proposed rule change so that it has sufficient time to consider the proposed rule change and the issues raised therein. Accordingly, the Commission . . . designates March 3, 2025, as the date by which the Commission shall either approve or disapprove, or institute proceedings to determine whether to disapprove, the proposed rule change."

GENSLER BOWS OUT, DEFIANT ON CRYPTO

In the last weeks of his tenure, SEC Chair Gary Gensler said in interviews that he had not changed his core beliefs about the cryptocurrency industry.

For one thing, Gensler claimed that "many in the crypto field are not complying with our time-tested laws." In an interview with Yahoo Finance, he asserted that many digital assets remain "highly speculative . . . You have to question what is their true use case; what is their value proposition?"[8]

And to CNBC, he said "this field, the crypto field, is highly speculative and has not been compliant with various laws, whether anti-money laundering, sanctions, or securities laws."[9]

When asked his thoughts on customized rules for digital assets that will likely be proposed by the incoming administration, Gensler said it was proper for a newly-constituted SEC to "make [the] next decisions." Yet when asked about President Trump's stated intention to create a U.S. bitcoin reserve, Gensler noted that the balance sheets of central banks are backed by their respective governments, "not by putting some digital asset in their reserves. It's not how any central bank around the world has thought about conducting monetary policy."

ENDNOTES:

[1] https://www.sec.gov/newsroom/press-release

s/2025-30.

[2]*See* https://www2.ca3.uscourts.gov/opinarch/233202p.pdf.

[3]*Id.*

[4]*See* https://assets.ctfassets.net/sygt3q11s4a9/4p9Lq2LQwHaTvZcZEcXVTK/bf521831ffae3d7c871f0ba13de44bdc/SEC_v._Coinbase__Opinion_and_Order_1.7.24.pdf.

[5]*Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024); https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf.

[6]*Id.*

[7]*See* https://www.sec.gov/files/rules/sro/nysearca/2025/34-102186.pdf.

[8] https://finance.yahoo.com/video/outgoing-sec-chair-gensler-talks-210558980.html.

[9] https://www.youtube.com/watch?v=TeXXHNwsoy4.

ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SYSTEM

By Michelle W. Bowman

Michelle Bowman is a member of the board of governors at the Federal Reserve. The following is edited from remarks that she gave on November 22, 2024, at the 27th Annual Symposium on Building the Financial System of the 21st Century: An Agenda for Japan and the United States, in Washington, D.C.

Discussions of artificial intelligence ("AI") inevitably center on two main points: risks and benefits. Both of these can be frustratingly vague and amorphous. Proponents of AI project its widespread adoption will be as momentous as the industrial age—radically improving efficiency, increasing labor productivity, and changing the world economy. Skeptics largely focus on the risks, noting that it may introduce new and unpredictable variables into the economy and the financial system, including new forms of cyber-risk and fraud.

It would be impossible to predict what the future holds for AI, or how its use and impact will evolve over time. But as the technology continues to mature, as new use cases evolve, and it is rolled out more broadly, we will almost certainly be surprised by how it is ultimately used.

Looking at the financial industry-specific implications of AI, it is helpful to consider not only how it may change the financial system, but also how regulatory frameworks should respond to this emerging technology. Are the existing frameworks sufficient? If not, how can regulators best balance the risks AI may pose to bank safety and soundness and financial stability with the need to allow for continued innovation?

Broader availability of generative AI and large language models have created headlines and spiking stock prices, but the financial services sector has been using AI for some time.[1] Over time, it has become clear that AI's impact could be far-reaching, particularly as the technology becomes more efficient, new sources of data become available, and as AI technology becomes more affordable.

DO WE NEED A DEFINITION OF AI?

Before discussing the implications of AI and regulatory policy approaches, we should ask whether we need a definition of AI. As it has advanced, the number and variety of definitions used to define AI have expanded.[2] Some definitions focus on the algorithms—like the use of machines to learn and reason in a way that simulates human intelligence. Others focus on the outputs—the ability to perform complex tasks normally done by humans. In 2021, an interagency request for information from federal banking regulators, including the Federal Reserve, sought comment on banks' use of AI, but notably avoided using any single definition. Instead, this request listed a few possible

use cases, features, and forms. These included the use of structured and unstructured data; the use of alternative data sources; voice recognition and natural language processing; the algorithmic identification of patterns and correlations in training data to generate predictions or categorizations; and "dynamic updating," where an algorithm has the capacity to update without human intervention.[3]

While each definition of AI may serve its own purpose in the context of how it is used, any single narrow definition can be criticized. A more generic definition runs the risk of oversimplifying the range of activities, use cases, and underlying technology. A definition that captures the variability of AI technology in a more granular way runs the risk of being unwieldy in its length, and obsolete in the short-term as new forms and use cases emerge.

Within this definitional question—of whether and how you define AI—lies a more important policy question: Specifically, for what purpose is a definition required? In the context of the financial system, the definition of AI may help to delineate how the regulatory system addresses it and establishes the parameters for how it can be used by regulated institutions. Other specific contexts could also be included, like third-party service providers that support banks or other financial services providers, or use by regulators in support of their mandates.

A definition helps regulators and regulated institutions understand the activities that are subject to rules and requirements by defining the scope. While this definitional question is important to establish clarity about the scope of what constitutes AI, it can also distract us from a more important point—what is the appropriate policy framework to address the introduction and ongoing use of AI in the financial system?

I have no strong feelings about the ideal or optimal definition of AI, and some version of the many definitions floating around are probably adequate for our purposes. At a minimum though, a definition must establish clear parameters about what types of activities and tools are covered. But before leaving the topic, I want to offer a cautionary note. A broad definition of AI arguably captures a wider range of activity and has a longer "lifespan" before it becomes outmoded, and potentially never becomes outdated. But a broad definition also carries the risk of a broad—and undifferentiated—policy response. This vast variability in AI's uses defies a simple, granular definition, but also suggests that we cannot adopt a one-size-fits-all approach as we consider the future role of AI in the financial system.

INNOVATION AND COMPETITIVENESS

Knowing that the technology and use of AI continues to evolve leads to the question of how it should be viewed by regulators, particularly in light of the need for innovation and the effect on competition.

Innovation

AI tools have the potential to substantially enhance the financial industry. In my view, the regulatory system should promote these improvements in a way that is consistent with applicable law and appropriate banking practices.

One of the most common current use cases is in reviewing and summarizing unstructured data. This can include enlisting AI to summarize a single report or to aggregate information from different sources on the same or related topics. The AI "output" in these cases may not directly produce any real-world action, but it provides information in a more usable way to assist a human. AI use cases

like this may present opportunities to improve operational efficiency, without introducing substantial new risk into business processes. In some ways, the joining of AI outputs with a human acting as a "filter" or "reality check" can capture efficiency gains and control for some AI risks. Similarly, AI can act as a "filter" or "reality check" on analysis produced by humans, checking for potential errors or biases.

AI tools may also be leveraged to fight fraud. One such use is in combatting check fraud, which has become more prevalent in the banking industry over the last several years. In a recent report, the Financial Crimes Enforcement Network noted that from February to August of 2023, there were over 15,000 reports received related to check fraud, associated with more than $688 million in transactions (including both actual and attempted fraud).[4] The growth in check fraud over the past several years has caused significant harm not only to banks and the perceived safety of the banking system but also to consumers who are the victims of fraudulent activity. The regulatory response to help address this growing problem has unfortunately been slow, lacking in coordination, and generally ineffective.

Could AI tools offer a more effective way for banks to fight against this growing fraud trend? We already have some evidence that AI tools are powerful in fighting fraud. The U.S. Treasury Department recently announced that fraud detection tools, including machine learning AI, had resulted in fraud prevention and recovery totaling over $4 billion in fiscal year 2024, including $1 billion in recovery related to identification of Treasury check fraud.[5] While the nature of the fraud may be different in these cases, we should recognize that AI can be a strong anti-fraud tool and provide significant benefits for affected bank customers.

If our regulatory environment is not receptive to the use of AI in these circumstances customers are the ones who suffer. AI will not completely "solve" the problem of fraud—particularly as fraudsters develop more sophisticated ways to exploit this technology. But it could be important if the regulatory framework provides reasonable parameters for its use.

Another often-discussed use case for AI in financial services is in expanding the availability of credit. AI is not the first technology with potential to expand access to credit for the "un-" or "underbanked." We have long viewed alternative data as a potential opportunity for some consumers, like those with poor or no credit history but with sufficient cash flow to support loan repayment.[6]

AI could be used to further expand this access, as financial entities mine more data sets and refine their understanding of creditworthiness. Of course, we also know that using AI in this context—in a way that has more direct impact on credit decisions affecting individual customers—also presents more substantial legal compliance challenges than other AI use cases.

AI also has promise to improve public sector operations, including in regulatory agencies. As I have often noted, the data relied on to inform the Federal Open Market Committee decision-making process often is subject to revisions after-the-fact, requiring caution when relying on the data to inform monetary policy.[7] Perhaps the broader use of AI could act as a check on data reliability, particularly for uncertain or frequently revised economic data, improving the quality of the data that monetary policymakers rely on for decision-making. Additional data as a reliability check or expanded data resources informed by AI could improve the FOMC's monetary policymaking by validating and improving the data on which policymakers rely.

While these use cases present only a subset of the possibilities for the financial system, they illustrate the breadth of potential benefits and risks of adopting an overly cautious approach that chills innovation in the banking system. Over-regulation of AI can itself present risks by preventing the realization of benefits of improved efficiency, lower operational costs, and better fraud prevention and customer service.

Effect on Competition

The regulatory approach and framework can also promote competition in the development and use of AI tools in the financial system.

An overly conservative regulatory approach can skew the competitive landscape by pushing activities outside of the regulated banking system or preventing the use of AI altogether. Inertia often causes regulators to reflexively prefer known practices and existing technology over process change and innovation. The banking sector often suffers from this regulatory skepticism, which can ultimately harm the competitiveness of the U.S. banking sector.

In the United States, we often think about the financial system based on the regulatory "perimeter." We view institutions within the scope of federal banking regulation (banks and their affiliates) as being "in the perimeter," while entities that operate under other regulatory frameworks (including money transmitters licensed under state law) are "outside the perimeter." Of course, the global financial system includes institutions that operate on a cross-border basis, and tools and approaches often permeate throughout the financial system once they have been deployed successfully in some other part of the system. But we know that the regulatory perimeter is permeable, and there is always the risk that activity pushed outside the perimeter can transmit risk back into the system even as the activities garner less scrutiny and regulation than banks. Put differently, the overly conservative approach may present only a façade of safety, masking underlying risks to the financial system and those who rely on it.

Of course, there are risks to being overly permissive in the AI regulatory approach. As with any rapidly evolving technology, supervision of its use should be nimble. Its users must make sufficient risk-management and compliance investments to conduct activities in a safe and sound manner, and in accordance with applicable laws and regulations. While the banking system has generally been cautious and deliberate in its AI development and rollout, others have not. When left improperly managed and unmonitored, it can result in unintended outcomes and customer harm. For example, certain generative AI models have been known to generate nonsensical or inaccurate outputs, sometimes called "hallucinations." In some cases, AI hallucinations have not involved significant harm, for example when discovered in a testing environment without customer-facing implications.

THE SUFFICIENCY OF EXISTING REGULATORY TOOLS

While helpful to acknowledge the risks of over-regulation and under-regulation, we must understand our currently regulatory stance—what tools do we have to promote AI's benefits while helping to mitigate the risks? To address this topic, we should widen the lens to consider our approach to innovation broadly. Supporting innovation in the financial system can and should apply to the introduction and use of AI.[8]

When we consider AI risks, many of these are already well-covered by existing frameworks. For example, AI often depends on external parties—

cloud computing providers, licensed generative AI technologies, and core service providers—to operate. AI can also pose model risks in the banking context, with associated data management and governance concerns. AI can also impact a bank's cyber-resiliency as AI-related fraud tools become more widespread and more anti-fraud tools become available.

While AI may be on the frontier of technology, it does not operate outside the existing legal and regulatory framework. AI is not exempt from current legal and regulatory requirements, nor is its use exempt from scrutiny. This is particularly true with AI; its use must comply with current laws and regulations, including fair lending, cyber security, data privacy, third-party risk management, and copyright. And when AI is deployed in a bank, an even broader set of requirements may apply depending on the use case.

Regulators are often playing "catch-up" with banks at the forefront of innovation. As a result, they often suffer from significant disadvantages in terms of understanding how the technology works, understanding the uses of AI within financial institutions, and keeping up-to-date with the latest AI developments. Of course, further compounding this challenge is that much of the work in AI innovation occurs far outside the banking system, including in the development and testing of generative AI models and in compiling the data sources on which to train the models.

Despite these challenges—and the understandable regulatory instinct to limit its use in the financial system—we must avoid this temptation. A few general principles should govern a coherent regulatory approach, which are the same principles that I apply to innovation generally.[9]

First, we must understand AI before we consider whether and how to change our regulatory approach. With respect to various internal use cases, the Board has published a compliance program that governs artificial intelligence.[10] One of the foundational elements for a successful approach to AI, and one mentioned in this plan, is the development and acquisition of staff expertise.

Many banks have increased AI adoption to an expanding number of use cases. As this technology becomes more widely adopted throughout the financial system, it is critical that we have a coherent and rational policy approach. That starts with our ability to understand the technology, including both the algorithms underlying its use and the possible implications—both good and bad—for banks and their customers.

In suggesting that we grow our understanding and staff expertise as a baseline, I acknowledge that this has been, and is likely to remain, a challenge. The Federal Reserve and other banking regulators compete for the same limited pool of talent as private industry. But we must prioritize improving our understanding and capacity as this technology continues to become more widely adopted.

Second, we must have an openness to the adoption of AI. We need to have a receptivity to the use of this technology and know that successful adoption requires communication and transparency between regulated firms and regulators. One approach regulators can use to reframe questions around AI (and innovation generally) is to adopt a posture that I think of as technology agnosticism.

We should avoid fixating on the technology, and instead focus on the risks presented by different use cases. These risks may be influenced by a number of factors, including the scope and consequences of the use case, the underlying data relied on, and the capability of a firm to appropriately manage these

risks. Putting activities together may be a helpful way to get a sense of broad trends (for example, the speed of AI adoption in the industry), but is inefficient as a way to address regulatory concerns (like safety and soundness, and financial stability). This may seem like an obvious point, but at times regulators have fallen prey to overbroad categorizations, treating a diverse set of activities as uniformly and equally risky.

This approach allows us to be risk-focused, much like we try to do with other forms of supervision, moderating intensity for low-risk activities, and increasing the intensity for higher-risk ones.

Of course, regulatory agencies do not operate in a vacuum, so we must also ask what type of coordination we need to ensure that we promote safe and sound adoption of AI, and address broader financial stability risks, both domestically and internationally. As a threshold matter, we need coordination both within each agency and among domestic regulators that play a role in the supervision and regulation of the financial system, which requires an environment of open sharing of information.

A posture of openness to AI requires caution when adding to the body of regulation. Specifically, I think we need a gap analysis to determine if there are regulatory gaps or blind spots that could require additional regulation and whether the current framework is fit for purpose. Fundamentally though, the variability in the technology will almost certainly require a degree of flexibility in regulatory approach.

CLOSING THOUGHTS

Artificial intelligence has tremendous potential to reshape the financial services industry and the broader world economy. While I have suggested in my remarks that we need not rush to regulate, it is important that we continue to monitor developments in AI and their real-world effects. In the long run, AI has the potential to impact many aspects of the Fed's work, from our role in supervising the payment system, to the important work we do promoting the safe and sound operation of banks and financial stability. AI may also play a growing role in monetary policy discussions, as the introduction of AI tools alter labor markets, affecting productivity and potentially the natural rate of unemployment and the natural rate of interest.

But as we engage in ongoing monitoring—and expand our understanding of AI technology and how it fits within the bank regulatory framework—I think it is important to preserve the ability of banks to innovate and allow the banking system to realize the benefits of this new technology.

ENDNOTES:

[1]In 2017, the Financial Stability Board was already considering the financial stability implications of AI and machine learning in financial services. See Financial Stability Board, "Artificial intelligence and machine learning in financial services: Market developments and financial stability implications," https://www.fsb.org/uploads/P011117.pdf (Basel: Financial Stability Board, November 2017).

[2]The National Artificial Intelligence Initiative Act of 2020, 15 U.S.C. § 9401(3) defines artificial intelligence as ". . . a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to-(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."

[3]*See* Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence,

Including Machine Learning, 86 Fed. Reg. 16837 (March 31, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf.

[4]Financial Crimes Enforcement Network, "Financial Trend Analysis: Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023, "(Vienna: Financial Crimes Enforcement Network, September 2024). https://www.fincen.gov/sites/default/files/shared/FTA-Check-Fraud-FINAL508.pdf.

[5]*See* U.S. Department of the Treasury, "Treasury Announces Enhanced Fraud Detection Processes, Including Machine Learning AI, Prevented and Recovered Over $4 Billion in Fiscal Year 2024, "news release, October 17, 2024.

[6]*See* Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency, "Interagency Statement on the Use of Alternative Data in Credit Underwriting," news release, December 12, 2019. https://www.federalreserve.gov/supervisionreg/caletters/CA 19-11 Letter Attachment Interagency Statement on the Use of Alternative Data in Credit Underwriting.pdf.

[7]*See* Michelle W. Bowman, "Perspectives on U.S. Monetary Policy and Bank Capital Reform," (speech at Policy Exchange, London, England, June 25, 2024), https://www.federalreserve.gov/newsevents/speech/files/bowman20240625a.pdf.

[8]*See* Michelle W. Bowman, "Innovation and the Evolving Financial Landscape," (speech at The Digital Chamber DC Blockchain Summit 2024, Washington, D.C., May 15, 2024), https://www.federalreserve.gov/newsevents/speech/files/bowman20240515a.pdf.

[9]*See* Bowman, "Innovation and the Evolving Financial Landscape."

[10]*See* Board of Governors of the Federal Reserve System, Compliance Plan for OMB Memorandum M-24-10 (Washington: Board of Governors, September 2024 https://www.federalreserve.gov/publications/files/compliance-plan-for-omb-memorandum-m-24-10-202409.pdf

FINTECH LAW REPORT: DECEMBER 2024/JANUARY 2025 REGULATION AND LITIGATION UPDATE

By Duncan Douglass, Jennifer Aguilar and Nate Tyre

Duncan Douglass is a partner and the head of the payment systems practice at the law firm Alston & Bird, LLP. Jennifer Aguilar is a counsel and Nate Tyre are senior associates at the same firm. www.alston.com.

REGULATORY DEVELOPMENTS

CFPB Issues Final Rule on Federal Oversight of Larger Nonbank Digital Payment Application Providers

On November 21, 2024, the Consumer Financial Protection Bureau (the "CFPB") issued a final rule on its supervision of larger nonbank participants in the digital payment application market ("Payment Application Supervision Rule").[1] Under the Payment Application Supervision Rule, designated Larger Participants are subject to the CFPB's ongoing supervisory and examination authority. A "Larger Participant" under the Payment Application Supervision Rule is a nonbank that (1) provides general-use digital consumer payment applications, (2) annually transacts at least 50 million consumer payment transactions in U.S. dollars, and (3) is not a small business concern based on the Small Business Administration's size standards.[2]

A nonbank provides a general-use digital consumer payment application by "providing a covered payment functionality through a digital payment application for consumers' general use in making consumer payment transaction(s)."[3] This includes the provision of payment functionality through

software programs that consumers generally use through personal computing devices, such as a mobile phone, smart watch, tablet, laptop computer, or desktop computer.[4] Payment functionality includes "[r]eceiving funds from a consumer for the purpose of transmitting them" or "[a]ccepting from a consumer and transmitting payment instructions" or providing a product or service that "[s]tores for a consumer account or payment credentials, including in encrypted or tokenized form; and [t]ransmits, routes, or otherwise processes such stored account or payment credentials to facilitate a consumer payment transaction."[5]

For purposes of determining the 50 million consumer payment transaction threshold, the Payment Application Supervision Rule only applies to U.S. dollar transactions.[6] The CFPB explains that this excludes transfers of digital assets, including cryptocurrency (*e.g.*, Bitcoin and stablecoins)[7] because the marketplace for digital currencies is rapidly evolving, and the agency would like to continue to "gather data and information regarding the nature of such transactions and the impact of digital assets transactions on consumers."[8] This is a shift from the Payment Application Supervision Rule's original proposal in November 2023, which set a lower threshold of five million transactions and included digital assets.[9]

A "consumer payment transaction" is the "transfer of funds by or on behalf of a consumer who resides in a state to another person primarily for personal, family, or household purposes."[10] A "consumer payment transaction" does not include:

- Electronic transfers of funds that are requested by a sender to a designated recipient that is sent by an international money transfer provider;
- A transfer of funds by a consumer that is linked to a consumer's receipt of a different form of funds, such as a transaction for foreign exchange; or that is a securities and commodities transfer that is excluded from the definition of "electronic fund transfer" under Regulation E;
- "A payment transaction conducted by a person for the sale or lease of goods or services that a consumer selected from that person or its affiliated company's online or physical store or marketplace, or for a donation to a fundraiser that a consumer selected from that person or its affiliated company's platform"; and
- "An extension of consumer credit initiated through a digital application that is provided by a person who is extending, brokering, acquiring, or purchasing the credit or that person's affiliated company."[11]

As compared to the proposal, the Payment Application Supervision Rule revises the definition of "consumer payment transaction" to include transactions that are made for consumers "who reside in" a state, instead of being for consumers that are "physically located" in a state, so when nonbanks provide a general-use digital consumer payment application to a consumer who does not reside in a state (such as a foreign national), the transaction will not be counted toward the threshold.[12] In making this change, the CFPB acknowledged that most market participants are more familiar with assessing where a consumer resides than determining a consumer's location during a consumer payment transaction, which can change between transactions, particularly with the use of mobile phones.[13] The rule also excludes payment transactions that merchants and marketplaces conduct through their own platforms, which diverges from the proposed rule which only excluded merchants and market-

places that operated prominently in their own name.[14] The Payment Application Supervision Rule also deviates from the proposal by excluding from the definition of "consumer payment transaction" extensions of consumer credit that are performed through a digital application and provided by a person who is "extending, brokering, acquiring, or purchasing" the credit.[15]

The Payment Application Supervision Rule states that a covered person must not be a small business concern.[16] Under the Small Business Act, a small business concern is one that is independently owned and operated, not dominant in its field of operation, and smaller than the size standards established by Small Business Administration in 13 C.F.R. § 121.[17] Due to the CFPB's level of resources available, the Payment Application Supervision Rule's exclusion of small businesses is meant to ensure that the CFPB focuses on larger entities without requiring all entities with covered consumer payment transactions to be subject to the agency's supervisory and examination authority.[18]

Under the Payment Application Supervision Rule, the CFPB expands its authority to allow the agency to examine Larger Participants for compliance with federal consumer financial laws, assess risks to consumers, and obtain information about the Larger Participant's activities and compliance systems.[19] Examinations can include reviewing policies, procedures, and business practices to identify potential violations.[20] The CFPB can also require periodic reporting, conduct on-site visits, and impose corrective measures or penalties for noncompliance.[21]

According to the CFPB, the Payment Application Supervision Rule will apply to seven undisclosed entities who the CFPB estimates to be Larger Participants, based on the agency's analysis of "confidential entity-level transaction information."[22] The Payment Application Supervision Rule's application is narrower in scope than its proposal as the CFPB originally estimated that the rule would cover 17 entities.[23]

The Payment Application Supervision Rule became effective on January 9, 2025.

You can access the Payment Application Supervision Rule here: https://www.federalregister.gov/documents/2024/12/10/2024-27836/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications.

CFPB Issues Circular on Unfair, Deceptive, or Abusive Acts or Practices in Credit Card Rewards Programs

On December 18, 2024, the CFPB issued a circular (the "Credit Card Rewards Circular") to give notice that it has identified certain practices of credit card companies operating rewards programs that could violate the prohibition against unfair, deceptive, or abusive acts or practices ("UDAAP") under the Dodd-Frank Act.[24] Rewards programs are a common feature to many credit cards that tend to be prominently marketed by card issuers, widely used by consumers, and play a major role in consumer choices on which cards to apply for and use for any given transaction. The Credit Card Rewards Circular underscores the CFPB's position that the UDAAP prohibition applies broadly to the design, marketing, and administration of credit card rewards programs. The CFPB asserts in the Credit Card Rewards Circular that covered rewards program operators may be liable for UDAAP violations even if the actions are attributable to a third party, like a merchant partner, and regardless of whether covered persons or service providers are taking actions consistent with rewards program terms.[25] While rewards program operators often retain the right to unilaterally modify credit card rewards programs, the CFPB asserts that some

modifications and actions may constitute UDAAP violations.

The CFPB identifies three categories of actions that may violate UDAAP prohibitions:

- *Devaluation of rewards that consumers have already earned*.[26] The CFPB explains that consumers often make decisions on whether to open or use a credit card based on the value of card benefits and rewards conveyed in a company's advertising and other communications. The CFPB argues that the devaluation of a consumer's accrued awards may be considered unfair or deceptive as it resembles a bait-and-switch scheme.[27]

- *Revocation, cancellation, or prevention of consumers' receipt of rewards based on buried or vague conditions*.[28] Fine print disclaimers or vague terms buried in a contract may conflict with prominent promotional language advertising the rewards that consumers can earn and "hinder a consumer's ability to make a 'free and informed choice.' "[29] As a result, the CFPB explains that consumers may not understand the vague or buried terms, which can cause monetary injury in the form of lost rewards value.

- *Failure to deliver earned rewards or the inability to redeem rewards*.[30] In offering rewards programs, operators make representations to consumers about how rewards can be redeemed and are ultimately responsible for administering the rewards program as represented. The CFPB explains that, when consumers lose points in the course of attempting to redeem rewards due to system failures, such issues may constitute deceptive or unfair practices because consumers have a reasonable basis to believe they were purchasing products or services with their points, which never occurred as a result of the system failure and consumers must often spend "significant time and resources trying to obtain [a] refund" of unredeemed points.[31]

In conjunction with the Credit Card Rewards Circular, the CFPB also issued a credit card report (the "Credit Card Report") identifying several issues of concern with retail credit cards. The Credit Card Report explains that retail credit cards are generally more expensive than general purpose credit cards, with higher annual percentage rates averaging 32.66% in December 2024 for new accounts.[32] Based on consumer complaints regarding retail credit cards, the CFPB also identifies issues with aggressive sales tactics at the point of sale, inability to redeem promotions, consumer confusion about the products they signed up for, and frustration with paper statement fees and late fees.[33] The CFPB suggested that the "heightened risks" in the retail credit card market deserve separate attention and stated that it will continue to monitor the market to ensure compliance with federal consumer financial laws.[34]

You can access the Credit Card Rewards Circular here: https://www.federalregister.gov/documents/2024/12/30/2024-30988/consumer-financial-protection-circular-2024-07-design-marketing-and-administration-of-credit-card?utm_campaign=subscription+mailing+list&utm_medium=email&utm_source=federalregister.gov.

You can access the Credit Card Report here : https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-the-high-cost-of-retail-credit-cards/.

CFPB Proposes Interpretive Rule Clarifying How the EFTA and Regulation E Applies to Emerging Payments

On January 10, 2025, the CFPB published an

interpretive rule and request for comment on the applicability of the EFTA and Regulation E to new and emerging forms of payments, fund transfers, and digital technologies ("Emerging Payments Interpretive Rule").[35] The Emerging Payments Interpretive Rule concludes that persons offering new methods to transfer funds should understand whether their account meets certain definitions in the EFTA and Regulation E and, therefore, are subject to regulatory compliance requirements.[36]

The Emerging Payments Interpretive Rule stems from the CFPB's research into emerging forms of payments, fund transfers, and digital technologies for "personal, family, or household purposes."[37] In 2021, the CFPB inquired into large technology firms' and digital payment applications' payments offerings, learning more about how these firms provide accounts for storing and transmitting funds.[38] A working group on financial markets also published a report in November 2021 discussing financial stability and concerns about bank and nonbank issuance of stablecoins, noting that laws and regulations (including the EFTA) protect consumers when using payments services.[39] Additionally, in April 2024, the CFPB published a report on the business practices of gaming platforms and game players' use of the platforms to convert U.S. dollars into virtual currency.[40]

In the Emerging Payments Interpretive Rule, the CFPB evaluates how emerging payment methods could be subject to the EFTA and Regulation E. Under the EFTA and Regulation E, an electronic fund transfer ("EFT") "generally means any transfer of 'funds' that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account."[41] In reviewing the definition of "financial institution," the CFPB explains that it includes "nonbank entities that directly or indirectly hold an account belonging to a consumer, or that issue an access device and agree with a consumer to provide EFT services."[42] Further, the CFPB asserts that the term "funds," which is not defined in the EFTA or Regulation E, is "broadly understood" to include more than just fiat currencies.[43] The CFPB claims that "funds" includes any "assets that act or are used like money," such as "stablecoins, as well as any other similarly-situated fungible assets that either operate as a medium of exchange or as a means of paying for goods or services."[44]

The CFPB also evaluates what constitutes an "account" under the EFTA and Regulation E, which is defined as a "demand deposit (checking), savings, or other consumer asset account . . . established primarily for personal, family, or household purposes."[45] The CFPB explains that "account" can include any account "into which funds can be deposited" with functionality similar to a checking or savings account, such as "paying for goods or services from multiple merchants, ability to withdraw funds or obtain cash, or conducting person-to-person transfers."[46] The CFPB claims this could include video game accounts, virtual currency wallets, and credit card rewards points accounts. Based on the CFPB's interpretations, persons offering these types of *accounts* through which consumers can conduct transfers must comply with the EFTA and Regulation E with respect to such account and transfers, including disclosing the terms and conditions of the accounts and EFT services, investigating and resolving errors, complying with limits on a consumer's liability for unauthorized EFTs, and providing periodic statements.

Comments on the Emerging Payments Interpretive Rule are due by March 31, 2025.

You can access the Emerging Payments Interpretive Rule here: https://www.federalregister.gov/doc

uments/2025/01/15/2025-00565/electronic-fund-transfers-through-accounts-established-primarily-for-personal-family-or-household.

LITIGATION AND ENFORCEMENT DEVELOPMENTS

Technology Trade Groups File Suit Against the CFPB Over Its Payment Application Supervision Rule

On January 16, 2025, technology trade groups TechNet and NetChoice, LLC (the "Tech Plaintiffs")[47] filed a lawsuit (the "Tech Group Complaint") against the CFPB, accusing the agency of arbitrarily and capriciously exceeding its authority in violation of the Dodd-Frank Act and Administrative Procedure Act ("APA") when it issued the Payment Application Supervision Rule.[48] The Payment Application Supervision Rule, issued by the CFPB on November 21, 2024, requires designated Larger Participants to be subject to the CFPB's ongoing supervisory and examination authority.[49] A "Larger Participant" under the Payment Application Supervision Rule is a nonbank that (1) provides general-use digital consumer payment applications, (2) annually transacts at least 50 million consumer payment transactions in U.S. dollars, and (3) is not a small business concern based on the Small Business Administration's size standards.[50]

In the Tech Group Complaint, the Tech Plaintiffs allege that the CFPB passed the Payment Application Supervision Rule in violation of the agency's statutory authority and without appropriately considering the rule's costs and benefits.[51] The Tech Plaintiffs assert that, under the Dodd-Frank Act, the CFPB's supervisory authority for nonbanks must be "risk-based" and that the CFPB exceeded its statutory authority because it referenced only speculative future risks that "may" occur, failed to identify any "actual harms or risks to consumers" in the target market and failed to find a "gap" in regulatory oversight as the financial products and services covered by the Payment Application Supervision Rule are already subject to supervisory oversight under state law.[52] The Tech Plaintiffs also allege that the CFPB exceeded its authority under the Dodd-Frank Act by applying its supervisory authority to "any consumer financial product[. . .] or service[. . . that is] offered by a covered company, so long as that company offers one product that qualifies for supervision[. . .]" rather than limiting its supervisory authority to the target market as required under the Dodd-Frank Act.[53] The Plaintiffs also claim that the Payment Application Supervision Rule is arbitrary and capricious, in violation of the Dodd-Frank Act and the APA, since the CFPB inappropriately identified the target market by "combining funds transfer functionalities and payment wallet functionalities" in the same "overly broad" market without making an "appropriate" cost-benefit analysis or considering important distinctions between such functionalities.[54] Given these deficiencies in the Payment Application Supervision Rule, the Tech Plaintiffs request that the court vacate and set aside the rule, declare that the CFPB exceeded its statutory authority, and enjoin the CFPB from taking action under the rule.

The case before the United States District Court for the District of Columbia is *TechNet et. al. v. Consumer Financial Protection Bureau et. al.*, Case No. 1:25-cv-00118. You can access the docket here: https://ecf.dcd.uscourts.gov/cgi-bin/DktRpt.pl?166051013683706-L_1_0-1.

CFPB Files Suit against Early Warning Services and Owner Banks Over Zelle Fraud

On December 20, 2024, the CFPB filed a lawsuit against Early Warning Services, LLC ("EWS"), Bank of America, N.A. ("BofA"), JPMorgan Chase

Bank, N.A. ("Chase"), and Wells Fargo Bank, N.A. ("Wells Fargo," collectively, the "Defendant Banks") accusing the defendants of failing to protect consumers from fraud that was perpetrated through the Zelle payments network ("Zelle Fraud Complaint").[55] The CFPB brought the lawsuit against EWS, as the operator of the Zelle network and the entity that establishes and oversees the Zelle network's rules, and against the Defendant Banks, as the largest participating financial institutions in the Zelle network and owners of EWS. In the Zelle Fraud Complaint, the CFPB claims that EWS and the Defendant Banks "rushed" Zelle to market to compete against burgeoning payment apps and without instituting effective anti-fraud safeguards or complying with consumer financial protection laws.[56] The CFPB alleges that, as a result of these actions, EWS and the Defendant Banks violated the Consumer Financial Protection Act ("CFPA") and engaged in unfair acts or practices.[57] The CFPB also alleges that the Defendant Banks violated the EFTA and Regulation E.[58]

The CFPB asserts that EWS and the Defendant Banks engaged in unfair acts or practices in violation of the CFPA by failing to prevent fraudulent use of the Zelle network. Specifically, the CFPB asserts that EWS violated the CFPA as it failed to implement effective fraud prevention measures, provide adequate information about payment recipients, and monitor and enforce the Zelle network rules.[59] The CFPB alleges that part of EWS's failure was in the design of the Zelle sign-up process, which the CFPB argues was intended to be "intentionally fast and frictionless" and which does not include sufficient fraud prevention measures or network rules to authenticate Zelle users' identities or verify their access to Zelle tokens.[60] The CFPB explains that EWS permits consumers to enroll in Zelle using their email address or phone number as a token, to associate multiple tokens to one bank account, to enroll at multiple financial institutions with different tokens, and to reassign tokens to other financial institutions.[61] The CFPB alleges that the Zelle network also allows a consumer to send money to another consumer by using the recipient's email address or phone number even if the recipient has not registered such email address or phone number with Zelle.[62] In that case, the recipient accesses the money by simply registering the token.[63] The CFPB claims that the ease of enrolling, registering, and reassigning tokens and the ability to receive funds to unregistered tokens allowed bad actors to perpetuate fraud on the Zelle network because the bad actors could frequently change tokens in order to avoid detection and register new tokens after receiving funds.[64] The CFPB also alleges that EWS failed to provide complete information to consumers about the identity of recipients before sending funds, which made it easier for bad actors to commit fraud by misrepresenting the recipient's identity or account ownership.[65] In supporting its position, the CFPB mentions various fraud schemes that were perpetrated through Zelle which resulted in both unauthorized fraud, such as account takeovers, and induced fraud, such as goods and services, romance, and impersonation scams.[66]

The CFPB also claims that EWS engaged in unfair acts or practices by "failing to take timely, appropriate, and effective network-wide measures to prevent, detect, limit, and address Zelle fraud."[67] The CFPB states that EWS did not appropriately provide risk-related information to financial institutions when the financial institutions paused or blocked a suspicious or risky transfer.[68] The CFPB also alleges that EWS did not appropriately require financial institutions to make timely, accurate reports about fraud, because such reporting was limited to disputes involving unauthorized fraud and did not include disputes related to induced fraud.[69] The CFPB alleges that EWS also did not

appropriately supervise and enforce the Zelle network rules against participating financial institutions, and EWS was aware that some financial institutions were violating the rules that EWS designed to protect against fraud.[70]

In the Zelle Fraud Complaint, the CFPB asserts that the Defendant Banks engaged in unfair acts or practices in violation of the CFPA by failing to implement effective fraud prevention measures, which included failures to properly authenticate Zelle users' identities during registration.[71] The CFPB also alleges that the Defendant Banks' failure to provide adequate information to consumers about the recipients of Zelle transfers, such as the full name of the recipient, and failure to suspend or restrict customers repeatedly accused of fraud from using Zelle constitutes unfair acts or practices by the Defendant Banks.[72] In discussing these alleged unfair acts and practices, the CFPB notes that the Defendant Banks' failures led to both unauthorized fraud and induced fraud.[73]

The CFPB alleges that the Defendant Banks failed to afford their consumers the protections required under the EFTA and Regulation E in connection with Zelle transfers.[74] The CFPB asserts that the Defendant Banks failed to reasonably investigate notices of errors related to unauthorized and incorrect transfers by reviewing only their internal records and not reviewing information held by EWS or by the other financial institutions involved in the Zelle transfer and instead relying only on "incomplete and non-dispositive information."[75]

Additionally, the CFPB asserts that when bad actors obtained an access device, such as a one-time passcode, phone, or laptop, via fraud or theft and used the access device to initiate a Zelle transfer, the Defendant Banks failed to treat such transfers as unauthorized and denied consumers' error claims.[76] The CFPB also alleges that BofA and Chase failed to "reasonably" investigate notices of errors involving transfers that were misdirected as a result of token directory errors and failed to treat such misdirected transfers as errors.[77]

According to the CFPB, the defendants' failures resulted in millions of complaints about fraud involving Zelle and over $800 million in fraud losses.[78] In seeking judicial relief, the CFPB has requested a permanent injunction on the defendants against further CFPA, EFTA, and Regulation E violations; monetary relief; a civil monetary penalty; costs against the defendants; and any additional injunctive or other relief the court finds necessary.[79]

The case before the United States District Court for the District of Arizona is *Consumer Financial Protection Bureau v. Early Warning Services, et al.*, Case No. 2:24-cv-03652-SMB. You can access the docket here: https://ecf.azd.uscourts.gov/cgi-bin/DktRpt.pl?10145095775846-L_1_0-1.

Google Payment Corporation Challenges CFPB Supervision Designation in Federal Lawsuit

On December 6, 2024, Google Payment Corporation ("GPC")[80] sued the CFPB in the U.S. District Court for the District of Columbia ("GPC Complaint"),[81] following the CFPB's assertion of supervisory authority over GPC ("CFPB Supervision Decision and Order").[82] GPC argues that the CFPB lacks a reasonable basis for exercising supervisory authority over GPC under the CFPA[83] because the CFPB relied on a small number of unsubstantiated complaints relating to consumer financial products and services that GPC has since retired from use to make its determination.[84] At the time the CFPB initiated the administrative process to designate GPC for direct CFPB supervision in March 2023, GPC had three relevant products in operation: (i) a peer-

to-peer payment product ("P2P"), (ii) a stored-value product known as Google Pay Balance, and (iii) a virtual Google Pay Balance Card for in-store and online merchant purchases. All three products were accessible through the Google Pay application ("Google Pay App") or Google Pay's web interface until they were retired on June 7, 2024.[85] GPC alleges that the CFPB's supervision designation (1) exceeds statutory authority, (2) is arbitrary and capricious, (3) failed to follow procedures required by law, and (4) is unsupported by substantial evidence.[86] GPC is seeking to have the designation vacated and set aside by the court.[87]

The CFPB's supervision designation is based on its use of a previously "dormant provision" of the Dodd-Frank Act and a related procedural rule issued by the CFPB in 2013[88] to "supervise nonbank financial companies where [the CFPB has] reasonable cause to believe that the company is posing risk to consumers."[89] In a blog post on May 5, 2022, the CFPB announced plans to use a "risk-based prioritization process" to determine which nonbank entities will be subject to supervisory examinations under this dormant provision.[90] In subsequent posts, the CFPB suggested it could use such authority to supervise tech companies in the consumer payments market.[91]

The GPC Complaint first claims that the CFPB exceeded its statutory authority under the CFPB in designating GPC for supervision because GPC's activities do not rise to a sufficient level of risk to support the designation. GPC refutes the CFPB's interpretation of the CFPA as authorizing a supervision designation of an entity engaged in "conduct that poses risks to consumers," without requiring a showing of material or substantial risk.[92] GPC argues that the CFPB's interpretation of its statutory authority would mean it has authority to supervise any entity that offers any consumer financial product or service, because the CFPB has previously acknowledged that all consumer financial products and services present some risk.[93] GPC further claims that the CFPB cannot base a supervision designation solely on past risks.[94] Following the June 2024 retirement of GPC's Google Pay App, the P2P payment product and Google Pay Balance stored value product are no longer available to consumers in the United States.[95] GPC claims that the decision to retire the products was not made to evade supervision,[96] and that following the retirement there is no current or future risk to consumers from these products or related services.[97] According to the GPC Complaint, the CFPB's expansive interpretation that it has authority to supervise any company creating any risk of any kind presents a number of constitutional issues.[98] GPC claims the interpretation intrudes on state regulations, violates the major questions doctrine by asserting authority Congress has not clearly granted it, and violates the non-delegation doctrine because the CFPB fails to identify an intelligible principle based on the statute to guide the CFPB's discretion in making supervision designations.[99]

GPC next alleges that the CFPB's determination to subject GPC to supervision is arbitrary and capricious on multiple grounds. GPC claims the CFPB failed to justify why its arguments were sufficient to meet statutory requirements and ignored contrary evidence presented by GPC.[100] For example, GPC indicates that it investigated the complaints identified in the CFPB's allegations of risks to consumers and provided explanations of the outcomes to the CFPB to demonstrate that GPC has sufficient policies and acted appropriately.[101] In addition, GPC provided evidence of its compliance program and argued that it is already subject to examination by state regulators.[102] According to GPC, the CFPB ignored this evidence.[103] GPC also alleges that the CFPB, throughout the administrative proceeding,

threatened GPC that the CFPB would publicize concerns about consumer risks of GPC products if GPC did not consent to supervision.[104] GPC alleges that the CFPB arbitrarily and capriciously changed its policy to allow public release of supervision designations in 2022 in order to use the threat of publicity to coerce companies into consenting to supervision, as the CFPB is doing with GPC.[105]

GPC alleges that the CFPB committed additional procedural violations in contravention of law in making its supervision designation. According to the GPC Complaint, the CFPB violated its own procedural rules by failing to articulate a discernible standard for how the CFPB was assessing the risk posed to consumers, failing to provide all bases for supervision in the initial Notice of Reasonable Cause, changing the bases for its designation throughout the administrative proceeding, and failing to explain the majority of evidence and documents on which the CFPB relied in its assessment of risk.[106] The CFPB cited 33 complaints in its supplemental brief that were not raised in the initial Notice of Reasonable Cause.[107]

Finally, GPC alleges in its complaint that the CFPB lacked evidentiary support for the supervision designation. The initial Notice of Reasonable Cause cited a lack of prior federal oversight of GPC and insufficient error resolution policies in violation of Regulation E.[108] GPC claims that the CFPB misread its error resolution policies and ignored the statutory requirement to give weight to state supervision.[109] GPC also alleges that the CFPB failed to identify sufficient evidence of conduct that poses risks to consumers.[110] The CFPB indicated it relied on 267 consumer complaints, 33 of which are described in the CFPB's supplemental brief.[111] The CFPB did not describe the details of its concerns relating to the other 234 complaints.[112] GPC also argues that 267 is an insufficient volume of complaints to be indicative of consumer risk when viewed in the context of the millions of P2P transactions that GPC processed in the relevant period.[113]

The case before the United States District Court for the District of Columbia is *Google Payment Corporation v. Consumer Financial Protection Bureau*, Case No. 1:24-cv-03419. You can access the docket here: https://ecf.dcd.uscourts.gov/cgi-bin/DktRpt.pl?275545.

Customers Sue Fintech Partner Banks After Synapse Failure

On November 22, 2024, and November 23, 2024, three separate class action complaints ("Partner Bank Complaints") were filed against Evolve Bank & Trust, Evolve Bancorp, Inc., AMG National Trust, Lineage Bank, and American Bank, Inc. (collectively, the "Partner Banks"), the banks that partnered with Synapse Financial Technologies, Inc. ("Synapse") in connection with Synapse's fintech product offerings.[114] The Partner Bank Complaints were filed by the customers of the fintechs who used Synapse to manage their customers' funds and account records.

According to the Partner Bank Complaints, Synapse opened deposit accounts on behalf of about 100 fintech companies and their customers at the Partner Banks and, in the wake of Synapse's bankruptcy in April 2024, it was discovered that about $85 million in customer funds across 100,000 customers were unaccounted for in the records of either Synapse or the Partner Banks.[115] In the Partner Bank Complaints, the plaintiffs allege that Synapse and the Partner Banks failed to maintain adequate records of customer funds and that the Partner Banks have failed to return all deposited funds, leaving many customers without access to their funds.[116] The plaintiffs further allege the Partner Banks were aware of the compliance issues

before Synapse's bankruptcy, failed to maintain contingency and business continuity plans for the potential failure of Synapse, and failed to maintain or obtain adequate records related to the deposited funds.[117] The plaintiffs allege that these facts support causes of action against the Partner Banks for money had and received, unjust enrichment, negligence, and conversion.[118]

The Partner Bank Complaints are before the United States District Court for the District of Colorado. You can access the dockets here: *Margul et al. v. Evolve Bank & Trust, et al.*, No. 1:24-cv-03259: https://ecf.cod.uscourts.gov/cgi-bin/DktRpt.pl?173812195818433-L_1_0-1, *Saquin et al. v. Evolve Bank & Trust, et al.*, No. 1:24-cv-03262: https://ecf.cod.uscourts.gov/cgi-bin/DktRpt.pl?15053645870531-L_1_0-1, and *Miller v. Evolve Bank & Trust, et al.*, No. 1:24-cv-03261: https://ecf.cod.uscourts.gov/cgi-bin/DktRpt.pl?18783454262113-L_1_0-1.

ENDNOTES:

[1]CFPB, *Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications*, (Nov. 21, 2024), https://www.federalregister.gov/documents/2024/12/10/2024-27836/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications.

[2]*Id.* at 99,584.

[3]*Id.* at 99,653.

[4]*Id.*

[5]*Id.*

[6]*Id.* at 99,612.

[7]*Id.* at 99,640.

[8]*Id.* at 99,588-589, 99,611.

[9]*Id.* at 99,583.

[10]*Id.* at 99,653.

[11]*Id.*

[12]*Id.* at 99,615.

[13]*Id.* at 99,612.

[14]*Id.* at 99,607, 99,615.

[15]*Id.* at 99,615.

[16]*Id.* at 99,584.

[17]*Id.* at 99,654; 15 U.S.C.A. § 632(a).

[18]Payment Application Supervision Rule, *supra* note 1 at 99,634.

[19]*Id.* at 99,582.

[20]*Id.* at 99,583.

[21]*Id.* at 99,646, 99,650

[22]*Id.* at 99,633, 99,639.

[23]*Id.* at 99,632.

[24]CFPB, *Consumer Financial Protection Circular 2024-07: Design, Marketing, and Administration of Credit Card Rewards Programs*, 89 Fed. Reg. 106277 (Dec. 30, 2024), https://www.federalregister.gov/documents/2024/12/30/2024-30988/consumer-financial-protection-circular-2024-07-design-marketing-and-administration-of-credit-card?utm_campaign=subscription+mailing+list&utm_medium=email&utm_source=federalregister.gov.

[25]*Id.* at 106,277.

[26]*Id.*

[27]*Id.*

[28]*Id.* at 106,280.

[29]*Id.* (*quoting F.T.C. v. Neovi, Inc.*, 604 F.3d 1150, 1158, 2010-1 Trade Cas. (CCH) ¶ 77012, 70 A.L.R. Fed. 2d 699 (9th Cir. 2010), as amended, (June 15, 2010); *American Financial Services Ass'n v. F.T.C.*, 767 F.2d 957, 976, 1985-2 Trade Cas. (CCH) ¶ 66702 (D.C. Cir. 1985)).

[30]*Id.* at 106,281.

[31]*Id.*

[32]*The High Cost of Retail Credit Cards*, CFPB Office of Markets (Dec. 18, 2024), https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-the-high-cost-of-retail-credit-cards/.

[33]*Id.*

[34]*Id.*

[35]CFPB, *Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Pay-*

ment Mechanisms, 90 Fed. Reg. 3,726 (Jan. 15, 2025), https://www.federalregister.gov/documents/2025/01/15/2025-00565/electronic-fund-transfers-through-accounts-established-primarily-for-personal-family-or-household.

[36]*Id.* at 3,727.

[37]*Id.* at 3,724.

[38]*Id.*

[39]*Id.* at 3,725.

[40]*Id.* at 3,724.

[41]*Id.* at 3,725.

[42]*Id.*

[43]*Id.* at 3,726.

[44]*Id.*

[45]*Id.* at 3,726.

[46]*Id.*

[47]Members of the trade groups include Amazon, Apple, Google, and PayPal.

[48]*TechNet et. al. v. Consumer Financial Protection Bureau et. al.,* No. 1:25-cv-00118. (N.D. D.C. Jan. 16, 2025).

[49]CFPB, *Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications*, 89 Fed. Reg. 99,582 (Nov. 21, 2024), https://www.federalregister.gov/documents/2024/12/10/2024-27836/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications.

[50]*Id.* at 99,584.

[51]Tech Groups Complaint *supra* note 48.

[52]*Id.* at 21-23, 26-27, 46-47.

[53]*Id.*at 47-48.

[54]*Id.* at 33-35, 49-51.

[55]*Consumer Financial Protection Bureau v. Early Warning Services, et al.*, No. 2:24-cv-03652-SMB (D. Ariz. Dec. 20, 2024).

[56]*Id.* at 3.

[57]*Id.* at 84-87.

[58]*Id.*

[59]*Id.* at 19-20.

[60]*Id.* at 12, 20.

[61]*Id.*

[62]*Id.*

[63]*Id.*

[64]*Id.* at 12-13.

[65]*Id.* at 23-24.

[66]*Id.* at 14.

[67]*Id.* at 78.

[68]*Id.* at 24, 79.

[69]*Id.* at 27, 79.

[70]*Id.* at 29-30, 79.

[71]*Id.* at 34, 46-47, 58.

[72]*Id.* at 37, 48-49, 60-61.

[73]*Id.* at 43, 54-55, 65-66.

[74]*Id.* at 67.

[75]*Id.* at 85-87.

[76]*Id.* at 73, 75.

[77]*Id.* at 71, 85-86.

[78]*Id.* at 4.

[79]*Id.* at 89-90.

[80]GPC is a subsidiary of Google LLC, which is a subsidiary of publicly traded corporation Alphabet, Inc.

[81]*Google Payment Corporation v. Consumer Financial Protection Bureau et al.*, No. 1:24-cv-03419, Doc. 1 (D.D.C. Dec. 6, 2024).

[82]*Google Payment Corporation v. Consumer Financial Protection Bureau et al.*, No. 1:24-cv-03419, Doc. 1-1 (D.D.C. Dec. 6, 2024).

[83]12 U.S.C. § 5514(a)(1)(C).

[84]GPC Complaint at 2, 29.

[85]*Id.* at 7.

[86]*Id.* at 34-39.

[87]*Id.* at 39.

[88]78 Fed. Reg. 40,352 (Jul. 3, 2013).

[89]Blog Post: *Explainer: What is nonbank supervision?*, CFPB (May 25, 2022), https://www.consumerfinance.gov/about-us/blog/explainer-what-is-nonbank-supervision/.

[90]*Id.*

[91]Interview of CFPB Director Rohit Chopra,

The Path Forward: Consumer Protection with Rohit Chopra, Lori Montgomery-The Washington Post (Apr. 11, 2023), https://www.washingtonpost.com/washington-post-live/2023/04/11/transcript-path-forward-consumer-protection-with-rohit-chopra/; Rohit Chopra, *Prepared Remarks of CFPB Director Rohit Chopra at the Brookings Institution Event on Payments in a Digital Century*, CFPB (Oct. 6, 2023), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-brookings-institution-event-on-payments-in-a-digital-century/.

[92] *Id.* at 22-23, 35; CFPB Supervision Decision and Order *supra* note 82 at 16; CFPA supra note 83.

[93]GPC Complaint *supra* note 81 at 23.

[94]*Id.* at 2, 24-25, 34.

[95]*Id.* at 5-7.

[96]*Id.* at 25.

[97]*Id.* at 24.

[98]*Id.* at 35

[99]*Id.* at 15, 22-23, 26-27, 35.

[100]*Id.* at 36-37.

[101]*Id.* at 19, 27-32.

[102]*Id.* at 7-9.

[103]*Id.* at 31-33.

[104]*Id.* at 4-5, 16.

[105]GPC Complaint *supra* note 81 at 14, 16, 36-37.

[106]*Id.* at 13-14, 16-18, 36-38.

[107]*Id.* at 16-18.

[108]*Id.* at 13; *see* 12 C.F.R. § 1005.11.

[109]GPC Complaint *supra* note 81 at 15, 32-33.

[110]*Id.* at 14.

[111]*Id.* at 2, 29-30.

[112]*Id.* at 29.

[113]*Id.* at 30.

[114]*Margul et al. v. Evolve Bank & Trust, et al.*, No. 1:24-cv-03259 (D. Colo. Nov. 22, 2024), https://ecf.cod.uscourts.gov/doc1/039011634646; *Saquin et al. v. Evolve Bank & Trust, et al.*, No. 1:24-cv-03262 (D. Colo. Nov. 23, 2024), https://ecf.cod.uscourts.gov/doc1/039011634819; *Miller v. Evolve Bank & Trust, et al.*, No. 1:24-cv-03261 (D. Colo. Nov. 23, 2024), https://ecf.cod.uscourts.gov/doc1/039011634646.

[115]*Id.*

[116]*Id.*

[117]*Id.*

[118]*Id.*

Editorial Board

FINTECH LAW REPORT

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

FIRST CLASS
MAIL
U.S.POSTAGE
PAID
WEST

FINTECH LAW REPORT

West LegalEdcenter
610 Opperman Drive, Eagan, MN 55123
Phone: 1-800-344-5009 or 1-800-328-4880
Fax: 1-800-340-9378
Web: http://westlegaledcenter.com

THOMSON REUTERS

YES! Rush me ***FinTech Law Report*** and enter my one-year trial subscription (6 issues) at the price of $1,020.00. After 30 days, I will honor your invoice or cancel without obligation.

Name _____

Company _____

Street Address _____

City/State/Zip _____

Phone _____

Fax _____

E-mail _____

METHOD OF PAYMENT

❑ BILL ME

❑ VISA ❑ MASTERCARD ❑ AMEX

Account # _____

Exp. Date _____

Signature _____

Postage charged separately. All prices are subject to sales tax where applicable.