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

May/June 2025 ▪ Volume 28 ▪ Issue 3

DOJ FINAL RULE APPLIES TO ANONYMIZED, PSEUDONYMIZED, AND DE-IDENTIFIED DATA: WHAT DATA LICENSORS NEED TO KNOW

By Julie A. Kilgore, Alexandra P. Moylan, Alisa L. Chestler and Dan S. Parks

Alicia Chestler is a shareholder, and Julie Kilgore and Dan Parks are associates, in the Nashville office of Baker Donelson. Alexandra Moylan is a shareholder in Baker Donelson's Baltimore office. Contact: jkilgore@bakerdonelson.com or amoylan@bakerdonelson.com or achestler@bakerdonelson.com or dparks@bakerdonelson.com.

What's Changed?

The U.S. Department of Justice ("DOJ") published a Data Security Program ("DSP"), pursuant to a final rule ("Final Rule"), which became effective on April 8, 2025. The DSP identifies prohibited and restricted transactions involving U.S. data access by countries of concern or by classes of covered persons. Unlike most privacy and data broker laws, the DSP does **not** exclude anonymized, pseudonymized, or de-identified data but rather expressly includes the foregoing within the definition of certain covered data.[1] This article focuses on the inclusion of anonymized, pseudonymized, and de-identified data within the scope of covered data, the broad applicability of the DSP, and the potential impacts on such data moving forward.

Who's Feeling the Impact?

Data licensors and other entities selling, licensing, or otherwise providing access to anonymized, pseudonymized, or de-identified data and entities using such data to develop or train artificial intelligence tools. The inclusion of data that is anonymized, pseudonymized, or de-identified expands the applicability and impact of the DSP to entities who may generally be exempted from complying with obliga-

IN THIS ISSUE:

Thomson Reuters™

43251760

tions under other laws with respect to these categories of data.

Why Should You Care?

Violations of the DSP include both civil and criminal penalties, and the U.S. Attorney General has determined that the prohibited and restricted transactions, including those merely involving anonymized, pseudonymized, or de-identified data, pose unacceptable risks to the national security of the United States. A U.S. Federal Trade Commissioner has also recently stated that a priority of the FTC will be to work closely with the DOJ to enforce the DSP, so monitoring and investigation are likely in this area.

What's Your Next Move?

Assess data license agreements and other agreements to determine whether data covered by the DSP, including any anonymized, pseudonymized, or de-identified derivatives of that data (or artificial intelligence tools trained with such data) are implicated. Next, assess whether the impacted agreements constitute a prohibited or restricted transaction. Finally, assess whether there is either access by, or any restrictions within the agreements to limit access by, a country of concern, a covered person, or any foreign person.[2]

Sensitive Data Now Includes Anonymized, Pseudonymized, and De-Identified Data

Unlike most privacy and data broker laws to date, the DSP is not solely or primarily concerned about the identifiability of the covered data at the point of access. The DSP defines one category of covered data (*i.e.*, bulk U.S. sensitive personal data) to mean a "collection or set of sensitive personal data relating to U.S. persons, in any format, **regardless of whether the data is anonymized, pseudonymized, de-identified**, or encrypted, where such data meets or exceeds the applicable threshold set forth [within the defined term 'bulk']." In contrast, for example, under most state privacy and data broker laws, personal data or personal information that meets the requisite standard of anonymization, pseudonymization, or de-identification is also exempt from the general requirements under the applicable law, except in limited circumstances (*e.g.,* basic contractual requirements). Additionally, under the Health Insurance Portability and Accountability Act and regulations promulgated thereunder ("HIPAA"), once covered data ("PHI") is de-identified in ac-

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

One Year Subscription ● 6 Issues ● $ 1020.00

cordance with the de-identification requirements set forth under HIPAA, the resulting data is no longer considered PHI and is exempt from most of HIPAA's requirements.

Broad Applicability

The DSP can apply to agreements beyond data licensing or similar data sharing agreements. For example, for covered prohibited transactions, the DSP prohibits the provision of access to both the data and an artificial intelligence tool that is merely capable of providing access to anonymized, pseudonymized, or de-identified data, even if access to such data is not explicitly provided. The DSP contains the following example to demonstrate this prohibition's intended applicability (**emphasis** added):

> A U.S. subsidiary of a company headquartered in a country of concern develops an artificial intelligence chatbot in the United States that is **trained** on the bulk U.S. sensitive personal data [including anonymized, pseudonymized, or de-identified data] of U.S. persons. While not its primary commercial use, the chatbot is **capable** of reproducing or otherwise disclosing the bulk U.S. sensitive personal health data that was used to train the chatbot when responding to queries. The U.S. subsidiary **knowingly** licenses subscription-based access to that chatbot worldwide, including to covered persons such as its parent entity. Although licensing use of the chatbot itself may not necessarily **''involve access''** to bulk U.S. sensitive personal data, the U.S. subsidiary knows or should know that the license **can be used to obtain access** to the U.S. persons' bulk sensitive personal training data if prompted. **The licensing of access to this bulk U.S. sensitive personal data is data brokerage** because it involves the transfer of data from the U.S. company (*i.e.*, the provider) to licensees (*i.e.*, the recipients), where the recipients did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. **Even though the license did not explicitly provide access to the data, this is a prohibited transaction because the U.S. company knew or should have known that the use of the chatbot pursuant to the license could be used to obtain access to the training data, and because the U.S. company licensed the product to covered persons.**

Due to restrictions on using identifiable information to train artificial intelligence tools, many entities have turned to using anonymized, pseudonymized, and/or de-identified data for such purposes. Therefore, licensing of such tools should also be carefully evaluated for potential implication under the DSP.

Future Impact

Because the DSP significantly deviates from the traditional approach with respect to anonymized, pseudonymized, and de-identified data, a key question that arises is whether this approach may be relied upon in future regulations or whether sensitive personal data will only be defined so broadly under laws addressing national security risks as opposed to those protecting against privacy risks. The commentary regarding the Final Rule contained a few nuggets that *may* preview changes to come, so entities regularly working with such data should continue to stay alert for future changes.

Intentional Inclusion

The lack of an exclusion for anonymized, pseudonymized, and de-identified data was not an oversight but an intentional deviation from the approach other laws have taken previously. Within the commentary of the Final Rule, the identifiability of data was flagged as only one of many concerns the DSP aims to address. Specifically, the commentary stated, "anonymized data is rarely, if ever, truly anonymous, especially when

anonymized data in one dataset can become identifiable when cross-referenced and layered on top of another anonymized dataset."

Additionally, "[a]nonymized data itself can present a national security risk, as can pattern-of-life data and other insights that harm national security from anonymized data itself." Finally, "advances in technology, combined with access by countries of concern to large datasets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data, allowing them to reveal exploitable sensitive personal information on U.S. persons." Thus, the potential for re-identification highlights a key reason the DSP explicitly applies to anonymized, pseudonymized, and de-identified data, not only identifiable data. However, the potential for re-identification is not new or unique to national security risks when transacting with these categories of data. The risk of re-identification is also present in many de-identified data transactions, often with contractual requirements being one of the few mechanisms, if not the only mechanism, for preventing re-identification of the data. Only time will tell whether re-identification risks that potentially impact national security will amount to more strenuous protection for individuals or if similar restrictions will be input within other privacy and data broker laws moving forward.

De-Identification Standards

The DSP includes restricted transactions that are permitted if entities comply with specified security requirements established by the Cybersecurity and Infrastructure Security Agency ("CISA"). The CISA data-level specifications generally require the implementation of mitigation techniques "sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern." While anonymization, pseudonymization, or de-identification of the data may be utilized in combination with other security requirements to achieve these specifications, all methods of such techniques permitted under other laws may not meet the CISA security requirements.

Commentary to the Final Rule suggests that the DOJ does not view all de-identification techniques as equal. The DOJ expressly confirmed its agreement with a commenter's recommendation to include de-identified PHI within covered data because "the HIPAA de-identification standards are out of date, and do not protect individuals in today's data-rich and computational-rich environment[. . .]" and the DSP should address "the ever-increasing ability to re-identify supposedly de-identified data." As a result, the DSP aims to strike a balance to allow restricted transactions that use robust anonymization, pseudonymization, or de-identification as specified by CISA's security requirements but prohibit the use of techniques that do not meet those standards. Therefore, for each restricted transaction, de-identification or similar techniques must be evaluated to determine if they meet CISA's data-level requirements. Again, it is unknown at this time whether the CISA standards or the criticisms of traditional techniques will be leveraged more broadly in the future.

ENDNOTES:

[1]An earlier Baker Donelson alert provides additional detail on the classes of transactions, countries, persons, and covered data. *See* https://www.bakerdonelson.com/doj-final-rule-targets-cross-border-data-transfers-key-implications-for-us-

and-foreign-owned-companies-operating-in-the-us.

[2]*See* our prior alerts related to next steps (https://www.bakerdonelson.com/doj-final-rule-targets-cross-border-data-transfers-key-implications-for-us-and-foreign-owned-companies-operating-in-the-us) and guidance (https://www.bakerdonelson.com/doj-issues-additional-guidance-and-clarification-on-the-bulk-data-transfer-rule-what-us-businesses-need-to-know) for additional compliance considerations.

OCC REVERTS TO PRIOR MERGER RULES

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 Office of the Comptroller of the Currency ("OCC") has issued an interim final rule[1] that restores streamlined and expedited regulatory procedures to review applications under the Bank Merger Act for business combinations involving national banks or federal savings associations.[2] It also rescinds a policy statement for OCC review of proposed bank merger transactions under the Bank Merger Act that sought to draw "chalk lines," demarcating the considerations and varying levels of scrutiny the OCC would use. The restored provisions are largely seen as pro-merger.

The OCC has restored the former regulatory provisions without any changes to them. The interim final rule became effective on May 15, 2025, upon publication in the Federal Register.[3] But the OCC is also accepting comments until June 16, 2025, and may issue a revised policy statement or guidance based on them.

We outline some considerations below for existing and potentially new national banks, as well as fintechs and crypto companies and non-U.S. banks.

Key Takeaways

The OCC has restored both **expedited review** (applications deemed approved 15 days after public comments, absent further OCC action) and **streamlined application procedures** for qualifying transactions under section 5.33 of the OCC's regulations without change.

- The 2024 final rule was criticized as deterring or disfavoring various mergers and transactions. With this change, the OCC is seeking to reduce the regulatory burden and uncertainty for market activity.
- The reversal effectively pivots from more subjective and ambiguous factors to more well established and neutral eligibility criteria.
- Under the restored provisions, there is less likelihood of a public meeting to delay various transactions.

By restoring these provisions, the OCC seeks to encourage economically beneficial combinations, which the industry may find helpful, particularly as compliance costs, deposit and other funding constraints, and interest rate and commercial real estate pressures have increased.

The policy shift is consistent with the Trump Administration's deregulatory policies, various executive orders, and recent similar policy changes at the FDIC.[4]

The interim final rule's comment period is an opportunity for national banks, bank holding companies, and other interested parties—includ-

ing fintechs and crypto companies—to suggest additional merger policy changes.

Considerations for Existing National Banks

The interim final rule notably reinstates automatic approval (after 15 days) **for internal business reorganizations**. Rather than taking a risk-based approach, the previous OCC leadership had posited than *any* business combination subject to a filing was a "significant corporate transaction" that required OCC approval. That approach was largely criticized as excessive and appeared emblematic of the Biden Administration's approach to bank regulation following the 2023 bank failures: seek to manage any and all risk by more uniformly applying the strictest scrutiny available in the regulatory toolbox.

In addition, various factors are no longer expressly applicable. Notably, being a global systemically important bank (or "GSIB"), or a subsidiary of one, will no longer be considered a *per se* transactional concern. Certain "positive" factors are also no longer codified, including that the target's combined total assets are less than or equal to 50% of acquirer's total assets and the resulting institution will have assets less than $50 billion. With the elimination of these subjective policies, banks of various sizes may consider more robust combinations.

Considerations for De Novo National Banks

By using a streamlined application—now once again available—applicants need not provide three years of financial projections for the merged institution.

The interim final rule reduces friction for organizers using interim banks in bank holding company formations, a common and relatively low-risk entry strategy. For instance, these combinations may rely on internal reorganization provisions. The elimination of the 2024 final rule no longer subjects them to heightened scrutiny under a vague "effect on communities" or "novelty" standard.

It also may facilitate startups' purchase of small, eligible banks and scale by, for instance, bringing tech and capital, but relying on the bank's existing infrastructure. These would not inherently trigger heightened scrutiny under the restored provisions and policy.

While also potentially leveraging a streamlined review process, these combinations will avoid subjective "novel" or "complex" standards that imposed full-scale merger review on startups.

Considerations for Fintechs and Crypto Companies

In addition to the above considerations, the interim final rule is seen as enabling eligible national banks, including **national trust banks**—an option used by various fintechs, crypto firms, and those involved in crypto-related activities—to restructure more easily. We expect that this flexibility will be a helpful consideration when picking a charter and thinking about future changes.

The relatively pro-merger changes are expected to better support fintech/crypto and other **acquisitions** of small OCC-chartered institutions using expedited tools, if capitalized appropriately. In addition, it changes ambiguous policy language that might have subjected **novel tech-bank** deals to subjective scrutiny by the OCC, especially for business models that included novel activities and technologies.

Considerations for Non-U.S. Banks

In addition to the above considerations, these relatively pro-merger changes make it easier for **U.S. subsidiaries or affiliates of foreign banks** to acquire eligible U.S. institutions to expand their U.S. operations.

The changes also support **streamlined filings** where foreign bank operations are expanding under existing U.S. charters.

ENDNOTES:

[1] https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-44.html.

[2]To simplify, we generally refer to "national banks" or just "banks" in this article.

[3] https://www.federalregister.gov/documents/2025/05/15/2025-08405/business-combinations-under-the-bank-merger-act-rescission.

[4] https://www.dwt.com/blogs/financial-services-law-advisor/2025/03/fdic-moves-to-rescind-controversial-bank-proposals.

NEW JERSEY FEDERAL COURT SIDES WITH KALSHI OVER PREDICTION MARKET CONTRACTS

By Johnny P. ElHachem

Johnny P. ElHachem is an associate in the Tallahassee and Miami offices of Holland & Knight LLP.
Contact: Johnny.ElHachem@hklaw.com.

Highlights

- Prediction market platform Kalshi has secured a preliminary injunction against the New Jersey Division of Gaming Enforcement preventing the state from enforcing a cease-and-desist order that aimed to halt Kalshi's operations within New Jersey.
- This legal action underscores the complex interplay between state and federal regulations in the realm of prediction markets.
- Though the ruling does not resolve the underlying legal issues, it marks yet another development for Kalshi and could serve as precedent for other federally regulated platforms confronting similar scrutiny.

Prediction market platform Kalshi has secured a preliminary injunction against the New Jersey Division of Gaming Enforcement (the "Division"), preventing the state from enforcing a cease-and-desist order that aimed to halt Kalshi's operations within New Jersey. This legal action underscores the complex interplay between state and federal regulations in the realm of prediction markets.

Background

Kalshi is a financial services company that operates a derivatives exchange and prediction market. It is registered with the Commodity Futures Trading Commission ("CFTC") as a Designated Contract Market ("DCM"), operating a federally regulated exchange where users trade contracts based on the outcomes of real-world events. Although Kalshi markets these products as financial instruments governed by the Commodity Exchange Act, some state regulators view them as a form of gambling, subject to state law.

In March 2025, the Division issued a cease-and-desist letter ordering Kalshi to cease its operations in the state, alleging that the platform's offerings constitute illegal gambling in violation of both the New Jersey Sports Wagering Act and New Jersey Constitution. In response, Kalshi filed suit in the U.S. District Court for the District of New Jersey, arguing that federal law preempts state enforce-

ment efforts and that New Jersey's actions violate the Supremacy Clause.

The Court's Decision

On April 28, 2025, the court found that Kalshi raised serious constitutional questions and demonstrated a likelihood of success and irreparable harm absent judicial intervention, and it enjoined the Division "from pursuing civil or criminal enforcement actions against Kalshi concerning its sports-related event contracts."

Notably, the court emphasized the tension between the state's interpretation of gambling laws and Kalshi's operation under federal regulatory approval. The court did, however, impose a $100,000 bond that was "intended to mirror that of the maximum fine of a violation [the Division could impose] under the New Jersey Sports Wagering Act."

Though the ruling does not resolve the underlying legal issues, it marks yet another development for Kalshi and could serve as precedent for other federally regulated platforms confronting similar scrutiny.

A Landscape in Flux: Federal and State Tensions Grow

The Kalshi-New Jersey dispute is just one front in a broader jurisdictional battle. In parallel, Kalshi has also been engaged in high-stakes litigation against the CFTC, challenging the agency's 2023 rejection of its proposed contracts tied to control of the U.S. Congress. A federal district court ruled in Kalshi's favor later that year, finding that the contracts were permissible under the Commodity Exchange Act. The CFTC initially appealed the decision to the U.S. Court of Appeals for the D.C. Circuit, but on May 5, 2025, it voluntarily dismissed the appeal, allowing the district court's pro-Kalshi ruling to stand.

That decision came just days after the CFTC abruptly canceled a long-anticipated public roundtable on event contracts that had been scheduled for April 30, 2025. The cancellation, coupled with the dropped appeal, has deepened uncertainty within the industry and raised broader questions about the Commission's posture, enforcement strategy, and willingness to clarify its regulatory approach to prediction markets.[1]

Kalshi Expands Legal Battle to Maryland

In a parallel development, Kalshi has initiated legal action against the Maryland Lottery and Gaming Control Commission following a cease-and-desist order similar to New Jersey's. Maryland authorities allege that Kalshi's event-based contracts violate state gambling laws. Kalshi contends that its operations fall under federal jurisdiction as a CFTC-regulated exchange and argues that Maryland's enforcement actions are preempted by federal law.

This marks Kalshi's third lawsuit against a state-level authority—having prevailed in Nevada by securing a preliminary injunction on April 9, 2025, against the Nevada Gaming Commission—highlighting the company's broader strategy to litigate its federal regulatory status across multiple jurisdictions.

In the absence of formal rulemaking or clear guidance from the CFTC, market participants are left to navigate an evolving legal landscape where both federal and state authorities assert overlapping—and sometimes conflicting—jurisdiction.

Implications for the Gaming Industry

For gaming operators, sportsbooks, financial

technology ("FinTech") companies and prediction market platforms, the Kalshi litigation underscores several key takeaways:

- **Preemption Is Not Automatic**. CFTC regulation provides a critical layer of federal authority, but it may not insulate platforms from state-level enforcement actions, particularly in jurisdictions with expansive definitions of gambling.
- **Multi-Forum Litigation Risk Is Real**. Platforms operating in this space must be prepared to defend their business models simultaneously in state courts, federal trial courts and before state and federal regulators.
- **Unsettled Law and Policy**. With the CFTC retreating from public engagement on these issues and key appeals pending, legal certainty remains elusive for operators seeking to structure novel event-based products.
- **Preliminary Injunctions Do Not Resolve the Merits**. Although Kalshi has obtained injunctive relief, these early rulings address only immediate harm and likelihood of success—not final adjudication. Courts may reach different conclusions as the cases advance.

Looking Ahead

Kalshi's wins in New Jersey and Nevada are far from the final word. As litigation continues in multiple jurisdictions—including the pivotal appeal in its challenge against the CFTC—market participants should proceed with caution.

Until clearer lines are drawn between permissible financial instruments and impermissible gambling contracts, businesses offering event-based products must invest in robust legal analysis, stay alert to shifting regulatory signals and be ready to litigate jurisdictional boundaries when challenged.

ENDNOTES:

[1]For more information about election and sports event contracts, *see* Holland & Knight's alert, "Election Contracts and Sports Event Contracts: The Future of Regulated Event-Based Trading," Feb. 11, 2025 (https://www.hklaw.com/en/insights/publications/2025/02/election-contracts-and-sports-event-contracts-the-future).

UK FCA DISCUSSION PAPER PROPOSES CRYPTO REGULATORY FRAMEWORK AND SEEKS INDUSTRY FEEDBACK

By Sebastian J. Barling, Simon Toms, Wilf Odgers and Cyrus Yazdanpanah

Sebastian Barling and Simon Toms are partners, Wilf Odgers is an associate, and Cyrus Yazdanpanah is a trainee solicitor in the London office of Skadden, Arps, Slate, Meagher & Flom LLP.
Contact: sebastian.barling@skadden.com or simon.toms@skadden.com or wilf.odgers@skadden.com or cyrus.yazdanpanah@skadden.com.

As part of the UK government's aim to create legislation establishing a regulatory framework for cryptoassets, on May 2, 2025, the UK Financial Conduct Authority ("FCA") published Discussion Paper DP25/1.[1]

The discussion paper covers key areas of the proposed new regulatory framework, including the potential impact on:

- Cryptoasset trading platforms ("CATPs").

- Cryptoasset intermediaries.
- Lending and borrowing in relation to cryptoassets.
- Staking and decentralized finance ("DeFi").

We outline some of the key points below.

The proposed framework will look familiar to many—it clearly builds off the existing approach used for traditional finance, and in particular the multilateral trading facility ("MTF") regime for CATPs and existing broker rules for intermediaries. The discussion paper is also cautious, reflecting the FCA's view that "cryptoassets will remain high-risk, speculative investments," and accordingly is more restrictive than other areas of financial regulation in terms of (in particular) the UK retail market, territoriality requirements and the need for UK-centric infrastructure.

The FCA is seeking feedback by June 13, 2025 to inform the next steps, which will be followed by a Consultation Paper. This is a relatively short time frame for participants to respond, particularly given the concurrent HM Treasury ("HMT") technical consultations on its proposed new statutory provisions to create new regulated activities for cryptoassets.

Cryptoasset Trading Platforms

Territoriality

The FCA has built on HMT's proposals to make it clear that entities operating a CATP in the UK will need to be authorized. In addition, overseas CATPs that serve UK retail customers will also need to be authorized, and this will require the establishment of a UK authorized firm.

However, the FCA has stated that it would like CATPs that provide services to UK retail clients to have an **authorized subsidiary in the UK**. This means a branch by itself will not be sufficient, given concerns around the veracity of home-state supervision as well as the ability for UK retail to trade directly on CATPs on an unintermediated basis.

The FCA has indicated that a model it is receptive to include an overseas firm establishing a UK branch for the purpose of running the matching engine and ensuring a singular liquidity pool, but with an affiliate UK-authorized subsidiary responsible for (broadly) client-facing and protection obligations.

In addition, authorization to operate a CATP through UK branches will only be given to an overseas firm on a case-by-case basis if it can meet the fundamental threshold conditions and general FCA expectations. A branch should only be authorized for non-UK firms, and not as a gateway to operate a predominantly UK business from an overseas jurisdiction.

A firm operating an offshore trading platform for cryptoassets that is only serving professional investors in the UK will not require FCA authorization. It is not intended to extend the overseas persons exclusion to cryptoassets.

As frameworks and cooperation among regulators mature, the discussion paper envisages the potential for greater reliance on overseas entities to carry out UK customer-facing regulated activities. That means branch-only models may become more palatable.

Participation in Trading Arrangements

The discussion paper proposes that CATPs be subject to additional rules and obligations where there is direct retail access, algorithmic or auto-

mated trading, and market-making activity. Regarding the operation of algorithmic trading and automated trading software, the FCA appears open to considering whether to adopt rules similar to those in traditional finance or develop alternative approaches.

CATPs should also identify entities operating market-making strategies, disclose potential conflicts and establish appropriate contractual agreements with them. It is possible that the scope of these rules may be limited to significant market-makers.

Trading and Execution

The FCA has indicated that all CATPs must operate nondiscretionary trading systems—*i.e.*, as per MTFs. This would mean a disapplication of best-execution requirements for those accessing CATPs directly.

The FCA has also indicated that it dislikes matched-principal trading, and that it favors a ban on operators of a CATP trading on their own platform, as well as the operator trading off-platform. The FCA is also skeptical about allowing entities affiliated with a CATP operator trading on the CATP, given the potential conflicts this can generate. However, the FCA is open to feedback on this position, especially in respect of affiliate principal trading.

Pre- and Post-Trade Considerations

The FCA has expressed concern around CATPs' involvement in:

- **Primary and secondary market activities**. The FCA is considering requiring legal (or functional) separation between a CATP and issuers of cryptoassets traded on that platform.
- **Internalizing and managing counterparty credit risk**. The FCA is keen to ensure that operators of CATPs are risk-neutral trading systems and therefore should be prevented from acting as a clearinghouse or extending credit to clients.
- **Settlement risk**. The FCA is considering the extent to which the operator of a CATP should be involved in managing settlement risk, but is receptive to views on the risks and market approaches.

Transparency

The FCA is proposing to impose both pre- and post-trade transparency requirements on CATPs; it would not impose pre-trade transparency waivers but is open to looking at (short) post-trade deferrals. In addition, CATPs will need to make their transparency data available to the public.

The FCA is not proposing to introduce a transaction reporting regime on CATPs but will require five years of transaction records to be kept. That said, the FCA is open to feedback as to how to best operationalize this requirement. The FCA is also keen to receive feedback on how to balance retail customer privacy with the need to have a personal identifier.

Cryptoasset Intermediaries

The discussion paper considers rules to regulate the conduct of intermediaries, following the principle of "same risk, same regulatory outcome" where possible.

The rules aim to address the risks and harms associated with intermediary activities such as consumer understanding, execution quality, order handling, and a lack of appropriate systems and controls.

The FCA is proposing to introduce the following investor protection measures in respect of order handing and execution:

- A requirement that any cryptoasset needs to be admitted to trading on at least one UK-authorized CATP before any intermediary can deal in it or arrange deals for UK retail customers.
- Extending the Consumer Duty to cryptoasset intermediaries.
- Requiring order execution procedures to be put in provide for the "prompt, fair an expeditious" execution of client order.
- Imposing MiFID-like best-execution standards, with a focus on "total consideration" as the key factor for retail clients, but with crypto-specific amendments, such as (i) potentially requiring an intermediary to check prices on at least three platforms, and (ii) limiting the ability to give specific instructions.
- Requiring orders for UK consumers to be executed on UK-authorized venues.
- Requiring additional disclosures to clients around trading capacity and order execution details.
- As per the position with CATPs, transaction reporting would not be required. Instead, record-keeping of client orders would be required for five years.

In respect of conflicts of interest, the FCA will expect firms to manage these as appropriate to their business model. However, the FCA identifies two specific types of conflicts it is concerned with for intermediaries:

- **Principal trading and client order execution**. The FCA expects firms to have as a minimum "functional separation" between principal trading and client order execution functions.
- **Payments for order flow**. Cryptoasset intermediaries will be prohibited from receiving payments for order flow.

In respect of the FCA's thinking on transparency requirements, it is proposing to impose post-trade transparency requirements on intermediaries, requiring the publication of details of executed transactions "as close to real-time as technically possible." The FCA is less developed in its approach to pre-trade transparency and welcomes views as to whether this should be introduced, and in what form.

In respect of client categorization by intermediaries, regulations in traditional finance allow retail customers to request to be "opted up" to become elective professional clients. The necessity of crypto-specific rules or guidance on retail customer opting-up practices is under consideration, with the FCA taking into account Consumer Duty guidance.

Cryptoasset Lending and Borrowing

The FCA proposes to have specific rules for cryptoasset lending and borrowing business models.

The key proposal is the banning of firms from offering cryptoasset lending and borrowing products to **retail clients**; the FCA is of the view that the volatility of cryptoassets makes them unsuitable for retail lending or borrowing.

However, the FCA has asked for feedback on proposed risk mitigation measures that could

make cryptoasset lending and borrowing more appropriate for retail clients. These are summarized in the table below.

Suggested Measures for Cryptoassets

Borrowing	Lending and Borrowing
Require firms to conduct creditworthiness checks and provide forbearance for those in or nearing arrears, in line with key Consumer Credit sourcebook rules.	Improve consumer understanding of cryptoasset lending and borrowing business models by introducing various requirements, such as express consent from consumers to firms before the contractual arrangement commences, as well as appropriateness assessments.
Require express consent from retail customers before collateral top-ups.	Restrict firms' use of their own platform tokens for cryptoasset lending and borrowing where there is a conflict of interest.
Limit how much a cryptoasset borrowing firm can automatically top up a consumer's collateral over the duration of the loan.	Restrict certain aspects of the cryptoasset lending and borrowing to only allow the use of qualifying stablecoins.

The FCA has proposed that institutional clients be permitted to access cryptoasset lending and borrowing products. This includes where a lender is facilitating lending and borrowing between different institutional clients.

Use of Credit To Purchase Cryptoassets

The FCA is exploring the appropriateness of restricting firms from accepting credit as a means for consumers to buy cryptoassets. A range of restrictions are under consideration, including those on the use of credit cards to directly buy cryptoassets, and using a credit line provided by an e-money firm to do so.

The initial expectation is that qualifying stablecoins from an FCA-authorized stablecoin issuer would be exempt from potential restrictions, and firms would not be restricted from offering credit options for the purchase of these qualifying stablecoins.

Staking

The FCA is concerned about a number of associated risks with staking, including technological, lack of consumer understanding and safeguarding. The table on the next page summarizes the key proposals for addressing these three risk categories.

Proposals To Mitigate Staking Risks

Technological	Consumer Understanding	Safeguarding
Make firms liable for financial losses suffered by retail consumers where the firm has inadequately assessed its technological and operational resilience, including third-party dependencies.	Prior to staking, firms must receive explicit consent from retail consumers on the amount of staked cryptoassets, conditions for payment, repayment, return of cryptoassets and fee-charging arrangements.	Firms should maintain: ▪ Separate wallets for consumers' staked cryptoassets, distinct from the firm's and other consumers' cryptoassets. ▪ Accurate records of staked cryptoassets at all times.
Require firms to implement robust arrangements as part of prudential requirements to ensure they hold sufficient capital to absorb losses, e.g., through slashing.	Retail consumers must receive key information on staking products and the associated risks in a key features document.	Firms will need to conduct regular reconciliations of staked cryptoassets.

Decentralized Finance

DeFi activities that could be considered "truly decentralized" would not be covered by the regime outlined in the discussion paper.

DeFi that involves the proposed regulated activities, and where there is a clear controlling person carrying on an activity, would be covered by the regime. This would include, for example, services that involve an identifiable intermediary or entity that has control over business operations and product features. The FCA would provide guidance to help firms understand their obligations and is seeking feedback on how to assess centralization and support compliance in the DeFi sector.

The discussion paper invites feedback on:

- How to assess the degree of centralization and decentralization.
- How decentralized features interact with the regulatory perimeter.
- Emerging industry practices that could support the implementation of the proposed regulatory obligations.

Crypto Road Map—Next Steps

In Q2 2025, the FCA will publish a consultation paper on the proposed rules and guidance for:

- Issuing a qualifying stablecoin.
- Safeguarding qualifying cryptoassets.
- Specified investment cryptoassets.

The consultation paper will be published alongside a second one on the prudential framework for cryptoassets and prudential requirements for qualifying stablecoins and safeguarding.

These activities will also be subject to wider conduct and firm standards, such as the Consumer Duty and rules within the Conduct of Business sourcebook. The FCA will consult on these standards in a third consultation paper on conduct and firm standards for regulated activities planned for Q3 2025.

Final Thoughts

The FCA's discussion paper helps drive the discussion around creating a UK crypto framework forward. However, the FCA proposals are cautious and prepared through the lens of (in particular) protecting retail customers; they will not fit neatly into many existing crypto business models and, if implemented as proposed, would require significant UK investment.

The FCA has indicated in most of the topics raised that it is amenable and keen to receive feedback as to how it can better tailor this regime to address its articulated concerns whilst also supporting growth. Firms should consider this an opportunity to weigh in before the regime is finalized.

This article is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice.

ENDNOTES:

[1] https://www.skadden.com/-/media/files/publications/2025/05/uk-fca-discussion-paper-proposes/regulating_cryptoasset_activities.pdf.

CRYPTO WATCH: THE TOKENIZATION DEBATE

On May 12, 2025, the Securities and Exchange Commission's Crypto Task Force held a roundtable whose debate topic was "Tokenization—Moving Assets Onchain: Where TradFi and DeFi Meet." Part of a series of SEC events being held this year on crypto asset regulation, the roundtable took place at the Commission's headquarters at 100 F Street in Washington, D.C. All of the SEC's current commissioners spoke at the event; the following is edited from their remarks.

Atkins: No More "Head in the Sand"

"It is a new day at the SEC," Chairman Paul Atkins said, in one of the first substantive policy speeches of his chairmanship.[1] "Policymaking will no longer result from ad hoc enforcement actions. Instead, the Commission will utilize its existing rulemaking, interpretive, and exemptive authorities to set fit-for-purpose standards for market participants." Atkins claimed the SEC's enforcement approach "will return to Congress' original intent, which is to police violations of these established obligations, particularly as they relate to fraud and manipulation."

Atkins observed that as securities increasingly migrate from traditional (or "off-chain") databases to blockchain-based (or "on-chain") ledger systems, this movement "from off-chain to on-chain systems" is akin to the transition audio recordings made starting in the 1970s, going from analog vinyl records to cassette tapes, compact discs to MP3s to streaming sites.

"The ability to easily encode audio in a digital file format, which could readily be transferred,

modified, and stored, unlocked tremendous innovation within the music industry," Atkins said. "Audio was freed from its boundaries as a static, fixed-format creation. It suddenly was compatible and interoperable across a wide range of devices and applications. It could be combined, broken apart, and programmed to form entirely new products. This also led to the development of novel hardware devices and streaming content business models, greatly benefiting consumers and the American economy."

The parallels to blockchain and crypto are obvious, he claimed. "The migration to on-chain securities has the potential to remodel aspects of the securities market by enabling entirely new methods of issuing, trading, owning, and using securities. For example, on-chain securities can utilize smart contracts to transparently distribute dividends to shareholders on a regular cadence. Tokenization can also enhance capital formation by transforming relatively illiquid assets into liquid investment opportunities. Blockchain technology holds the promise to allow for a broad swath of novel use cases for securities, fostering new kinds of market activities that many of the Commission's legacy rules and regulations do not contemplate today."

Noting that President Trump wants the U.S. to be the "crypto capital of the planet,"[2] Atkins claimed that it's necessary for the Commission to keep pace with innovation. This could mean rewriting some rulebooks, he said. "Rules and regulations designed for off-chain securities may be incompatible with or unnecessary for on-chain assets and stifle the growth of blockchain technology."

Atkins said one of his key priorities as Chairman will be to "develop a rational regulatory framework for crypto asset markets that establishes clear rules of the road for the issuance, custody, and trading of crypto assets while continuing to discourage bad actors from violating the law. Clear rules of the road are necessary for investor protection against fraud—not the least to help them identify scams that do not comport with the law." He praised the formation of the Crypto Task Force this past January, claiming that "for too long, the Commission has been plagued by policymaking siloes. The Crypto Task Force exemplifies how our policy divisions can come together to expeditiously provide long-needed clarity and certainty to the American public."

Atkins then delved into what he defined as the three main areas of focus for upcoming SEC crypto asset policy: issuance, custody, and trading.

Issuance

Atkins intends for the Commission "to establish clear and sensible guidelines for distributions of crypto assets that are securities or subject to an investment contract. Only four crypto asset issuers have conducted registered offerings and offerings pursuant to Regulation A. Issuers have largely avoided these types of offerings, in part, due to challenges in satisfying the associated disclosure requirements. In cases where the issuer does not intend to distribute ordinary securities, such as stock, bonds, or notes, issuers also struggle to determine whether a crypto asset constitutes a "security" or is subject to an investment contract."

In the past decade, the SEC pursued "what I call the 'head-in-the-sand' approach—perhaps hoping that crypto would go away," Atkins claimed. "Then it pivoted and pursued a shoot-first-and-ask-questions-later approach of regulation through enforcement. It claimed that it was willing to talk to prospective registrants, 'Just come in to visit,'

but this proved ephemeral at best and more often misleading because the SEC made no necessary adaptations to registration forms for this new technology."

As an example, Atkins listed Form S-1, which "continues to require detailed information regarding executive compensation and use of proceeds, which may not be relevant or material for investment decisions in crypto assets. While the SEC has previously adapted its forms for offerings of asset-backed securities and by real estate investment trusts, it has not done so for crypto assets despite increased investor interest in this space over the past few years. We cannot encourage innovation by trying to fit a square peg into a round hole."

The SEC will chart a new course, he claimed. One early step was the Commission's issuance of a statement on disclosure obligations for certain registrations and offerings,[3] and a clarification of the view "that certain distributions and crypto assets do not implicate the federal securities laws, and I expect the staff to continue to provide clarifications at my direction with regard to other types of distributions and assets."

"However, existing registration exemptions and safe harbors may not be entirely fit-for-purpose for certain types of crypto asset offerings," Atkins said. "I view this construct of staff pronouncements as extremely temporary—Commission action is both vital and necessary." In the meantime, Atkins has asked Commission staff "to consider whether additional guidance, registration exemptions, and safe harbors are needed to create pathways for crypto asset issuances within the United States. I believe that the Commission has broad discretion under the securities acts to accommodate the crypto industry, and I intend to get it done."

Custody

Atkins supports "providing registrants with greater optionality in determining how to custody crypto assets." For example, Commission staff recently removed what he described as a "significant impediment for companies seeking to provide crypto asset custodial services" by rescinding Staff Accounting Bulletin No. 121.[4] Atkins called that Bulletin "a grave error . . . the staff had no place to act so broadly in place of Commission action and without notice-and-comment rulemaking. The action created needless confusion and went far beyond the jurisdiction of the SEC in its effects. However, the SEC can do much more to enhance competition in the market for legally compliant custodial services than merely getting rid of SAB 121."

"It is important to provide clarity on the types of custodians that qualify as a 'qualified custodian' under the Advisers Act and Investment Company Act, as well as reasonable exceptions from the qualified custody requirements to accommodate certain common practices within crypto asset markets," he added. "Many advisers and funds have access to self-custodial solutions that incorporate more advanced technology to safeguard crypto assets as compared to some of the custodians in the market. Consequently, the custody rules may need to be updated to allow advisers and funds to engage in self-custody under certain circumstances."

Atkins also said it "may be necessary to repeal and replace the 'special purpose broker-dealer' framework[5] with a more rational regime." He noted that only two special purpose broker-dealers are in operation today, "due clearly to the significant limitations imposed on these entities. Broker-dealers are not and never were restricted from act-

ing as a custodian for non-security crypto assets or crypto asset securities, but Commission action may be needed to clarify the application of the customer protection and net capital rules to this activity."

Trading

Atkins is in favor of allowing registrants to trade a broader variety of products on their platforms and conduct activities, "which previous Commissions had prevented." For example, he said, "some broker-dealers seek to go to market with a "super app" that offers trading in securities and non-securities and other financial services all under a single roof. Nothing in the federal securities laws prohibits registered broker-dealers with an alternative trading system from facilitating trading in non-securities, including via "pairs trading" between securities and non-securities." He said SEC staff has been charged with finding ways to modernize the ATS regulatory regime "to better accommodate crypto assets [and] to explore whether further guidance or rulemaking may be helpful for enabling the listing and trading of crypto assets on national securities exchanges."

As the SEC works to develop what Atkins described as a comprehensive regulatory framework for crypto assets, "securities market participants should not be compelled to go offshore to innovate with blockchain technology," he said. "I would like to explore whether conditional exemptive relief would be appropriate for registrants and non-registrants that seek to bring new products and services to market that may otherwise not be compatible with current Commission rules and regulations." The goal is nothing less than making "the United States the best place in the world to participate in crypto asset markets."

Crenshaw: The Skeptic

Commissioner Caroline Crenshaw remains the SEC's house skeptic when it comes to cryptocurrency. In her remarks at the roundtable, she compared "the current enthusiasm around tokenization" to the famous line in the film *Field of Dreams*: "if you build it, they will come."[6]

"There is an argument that if we 'build'—or more accurately, 'rebuild'—the financial system to accommodate blockchain, 'they'—all manner of market participants—'will come' to embrace tokenized securities. Investors will benefit from increased participation and choice, and markets will flourish from blockchain-derived improvements," she said.

"To this, I would first ask, what exactly are we trying to build? What is tokenization? It is a term that, even limited to the SEC space, eludes a straightforward definition. Does tokenization mean issuing a security directly on a blockchain? Or does it refer to creating a digital representation of a security on a blockchain? This may seem a subtle distinction, but it likely carries significant consequences from a regulatory perspective. Beyond issuance, does or should tokenization encompass downstream distribution, trading, clearing and settlement? In other words, would the entire securities lifecycle move "on-chain," or only a part of it?"

Crenshaw claimed that however the SEC may try to answer such definitional questions, "it's clear that a tokenized financial system is unlike anything we've seen before . . . The vision many espouse seems to be a fully tokenized system, where any security, including high-volume liquid products like Fortune 500 stocks, can be issued, traded, cleared and settled on the blockchain."

She further questioned whether such a system is even technologically possible. "If we are talking about public permissionless blockchains, the answer at least of today seems to be no. The transaction volume limitations and other scalability problems are well understood. The whole concept of public permissionless blockchains—which were designed to provide trust without the need for government oversight—seems an awkward vehicle for something as complex and statutorily regulated as the securities markets."

If the SEC is talking about private or permissioned blockchains, even if that does improve the potential for scalability, "is this qualitatively different from other types of database technologies already in widespread use? Does it warrant any regulatory adjustments at all?"

Crenshaw further questioned why the SEC should "assess particular forms of blockchain as candidates for industry adoption? Why would we focus on blockchain in particular over other types of distributed ledger technologies? Regulatory efforts to facilitate adoption of blockchain, let alone specific forms of it, seem like the government picking winners and losers. And we seem to be doing so before the technology has even been demonstrated as fit for purpose."

The question lies not only in defining "what" the SEC is trying to build, but why the Commission is trying to build it, she said. "Proponents argue tokenization can speed up the settlement of trades and make markets more efficient. Instead of our current settlement cycle of T+1, tokenization could potentially move us to instant settlement or 'T+0.' There is also an argument that instant settlement could reduce counterparty risks because trades would be pre-funded. But the settlement cycle, while shorter than it used to be, is a design feature, not a bug. The intentional delay built in between trade execution and settlement provides for core market functionalities and protection mechanisms."

For example, the settlement cycle facilitates netting, she said. "Roughly speaking, netting allows counterparties to settle a day's worth of trades on a net basis rather than trade-by-trade. The sophisticated, multilateral netting that occurs in our national clearance and settlement system drastically reduces the volume of trades requiring final settlement. On average, 98% of trade obligations are eliminated through netting. This allows the current system to handle tremendous volume. It's a key reason why our markets withstood sustained, record-breaking trade volume in recent weeks without major failures."

Further, netting facilitates liquidity, Crenshaw claimed. "Because the vast majority of trades are "netted" and don't require settlement, they don't require an exchange of money. If A sells to B, B sells to C, and C sells to A, these trades are paired off and eliminated. A, B, and C can each retain their capital, as compared to a bilateral instant settlement over a blockchain, where each would have given up its cash for at least some period of time. Another important consideration is that instant settlement would generally disfavor retail investors, many of whom currently rely on the ability to submit payment after placing orders." Also, the settlement cycle is typically where regulators can assess potential fraud and cybercrime activities. "When red flags go up, the ability to pause a transaction and investigate is essential for investor protection and broader concerns like national security and counterterrorism."

To Crenshaw, "for these and other reasons, it is not at all clear that shortening the existing settle-

ment cycle is desirable or feasible . . . I think it is our statutory obligation as a regulator to exercise extreme caution with potential changes of this scale, which historically have been undertaken only to address true market crises. While there are certainly areas to improve in our markets, I am interested in whether the changes discussed today would fix any specific existing dysfunction."

She warned that "the kinds of systemic changes we're talking about have the potential to affect every market participant from Wall Street to Main Street. Let's ensure that what we're contemplating is appropriately scoped to the portion of the market that participates in crypto—recently estimated to be less than 5% of U.S. households—and not detrimental to the "TradFi" markets on which most Americans depend for their financial well-being."

Peirce: Tokenization Needs Clarity

By contrast, Commissioner Hester Peirce has been regarded as the Commission's advocate for the advancement of crypto. At the roundtable, she claimed that "tokenization is rooted in the internet . . . at the base of these networks are software protocols—a set of rules defining how computers and other devices communicate with each other. Protocols built on top of TCP/IP—the protocol that governs the internet—enable applications that facilitate communication and easy access to information."[7]

Blockchain and other distributed ledger technology protocols are new internet-based protocols enabling the creation of new global networks, this time to facilitate the seamless transfer of assets and related data. These protocols commonly rely on cryptography for their operation and security. Novel crypto assets that would not exist but for the underlying protocols live on these networks. So do traditional assets when they get tokenized. Tokenization fits squarely within the Commission's jurisdiction because it involves formatting traditional financial assets, like stocks and bonds, as crypto assets (or "tokens") on a crypto network. Much as earlier internet-based protocols dramatically enhanced our lives by making it easier to communicate and access information, these cryptographic protocols have the potential to improve our lives through enhanced accessibility and efficiency of the markets for traditional financial assets."

Much as how a "smartphone" enables a user to have access to a greater variety of information via its connection to the internet and its network of applications, "similarly tokenizing traditional assets and putting them on crypto networks makes them smarter," she said. "Crypto networks are not only a new type of database or ledger for recording ownership of assets, but also a new type of computing platform that can support applications that allow you to do more with your assets."

Further, "smart contracts are self-executing software programs that define important properties of assets and applications running on crypto networks and serve as a portal to the networks of applications supported by these new internet-based protocols. A smart contract can define how and when securities may be purchased, sold, and transferred, as well as automate dividend and interest payments or other distributions. Further, because of the common protocols used to program these smart contracts and the related assets and applications, investors can use tokenized securities seamlessly on or within other smart contract-based applications, including DeFi applications."

Removing securities from siloed databases and tokenizing them on open, composable crypto

networks "mobilizes them and makes them usable in new and enhanced ways," Peirce claimed. "Stablecoins, the first application of tokenization to achieve scale, demonstrate the efficiency and accessibility improvements that may arise from the use of crypto networks. Tokenization may provide similar benefits to the securities markets, such as increased operational efficiency, transactional transparency, liquidity, and accessibility; faster settlement; and greater investor opportunity."

For example, several tokenized money market products are registered under the Investment Company Act of 1940, "and tokenized private funds similarly issue securities designed to maintain a stable value and provide yield," she said. "Using crypto networks to maintain the record of ownership enables the securities to be used as collateral in derivatives transactions, rather than requiring investors to redeem the securities and then post cash as collateral. Tokenized securities also may serve as a means of settlement in the purchase and sale of other crypto assets, including other tokenized securities, in peer-to-peer or other types of on-chain transactions. If these assets live on the same network, near-instant and simultaneous settlement is possible."

Peirce noted that tokenization "cannot reach its full potential without legal clarity." Issuers and transfer agents remain unsure as to whether a crypto network can be the master securityholder file or a component thereof for purposes of the Exchange Act's transfer agent rules, even where state law expressly contemplates the use of a crypto network in connection with the maintenance of the securities ownership record.

"Further, the Commission's Special Purpose Broker-Dealer statement, which defines 'crypto asset security' to encompass any security that relies on cryptographic protocols, has created confusion regarding a broker-dealer's ability to custody tokenized traditional securities, even when issuers and transfer agents retain control and can address erroneous or impermissible transactions," she said. "The Commission proposed to amend the Advisers Act custody rule to preclude traditional securities that are issued on a public, permissionless crypto network from eligibility for an exception from the qualified custodian requirement."

Tokenization may raise legal challenges, she said. Some may be related, for example, to "integration with DeFi, application of the transfer agent rules and National Market System requirements, use of permissionless networks, and appropriate classification as certificated versus uncertificated securities." The SEC's Crypto Task Force is "working on providing legal clarity to these and other questions in a sensible manner," she said.

But "absent a compelling reason grounded in fact and law, the Commission should treat tokenized securities the same as traditionally issued securities. Under this approach, for example, the type of database used to record ownership of securities does not affect the substance of the securities issued, nor does the use of a crypto network give rise to a new or different type of security," she said. "A crypto network can constitute all or part of the issuer's books maintained by its transfer agent. Tokenized mutual fund shares and tokenized privately issued securities should be eligible for the exceptions for such securities from the Advisers Act qualified custodian requirement."

Uyeda: Time to Accommodate New Technologies

Commissioner Mark Uyeda argued that the

SEC "should not shy away from policymaking about emerging technologies, simply because it does not fit into the existing regulatory framework. The first step in sound policymaking is seeking input from market participants. In recent history, we seem to have forgotten a very fundamental concept: that investors and issuers have valuable observations and experiences."[8]

In this case, "market participants should not be left guessing as to how they can comply with the Commission rulebook. These roundtable conversations are a useful step in obtaining this information—with a view to constructing a regulatory framework that provides transparency and predictability for market participants that seek to bring assets onchain."

He said "developments related to the tokenization of real-world assets using blockchain technology implicate major financial market functions and processes like issuance, trading, transfer, settlement, and record of ownership. In addition to these potential market improvements, tokenization presents opportunities to expand the landscape to demonstrate proof of ownership—making possible new types of uses, such as tokens that represent title to real estate or holdings of intellectual property rights."

"These implications can potentially benefit investors by enhancing liquidity for otherwise relatively illiquid assets, reducing delays associated with intermediation, and also decreasing transactional costs," he said. Further, technology has the potential "to simplify, or at least streamline, certain compliance functions, such as through smart contracts for onchain assets. These potential improvements in capital markets are tied to key characteristics of blockchain technology. Blockchain technology relies on a transparent ledger and does not require a central intermediary. Market transparency impacts transactional costs, but also implicates potential compliance costs—as more opaque and complex markets may increase compliance costs."

For example, Uyeda said, "there are many challenging regulatory questions that the Commission and its staff may need to resolve under the regime established by Regulation NMS as securities move onchain. As such, we should evaluate whether these technologies can benefit all market participants."

Uyeda noted that then-SEC Commissioner Joseph Grundfest in the mid-1980s described a profound disconnect between Commission regulatory tools that were developed during the Great Depression and the many technological developments of the Reagan era. Uyeda implied that a similar disconnect exists at present.

"As we consider the implications of new technologies, we should design a framework that focuses on critical safeguards rather than trying to address every conceivable investment permutation and scenario . . . the same principles that helped regulation move from paper certificates to electronic recordkeeping and from faxes to texts can similarly guide us to accommodate new technologies."

ENDNOTES:

[1] https://www.sec.gov/newsroom/speeches-statements/atkins-remarks-crypto-roundtable-tokenization-051225.

[2] https://apnews.com/article/donald-trump-bitcoin-cryptocurrency-stockpile-6f1314f5e99bbf47cc3ee6fc6178588d.

[3] *See* Division of Corporation Finance, Offerings and Registrations of Securities in the Crypto

Asset Markets, Apr. 10, 2025, *available at* https://www.sec.gov/newsroom/speeches-statements/cf-crypto-securities-041025. Staff statements represent the views of the staff, and the Commission neither approved nor disapproved their content.

[4]*See* Staff Accounting Bulletin No. 122, Release No. SAB 122, Jan. 23, 2025, https://www.sec.gov/rules-regulations/staff-guidance/staff-accounting-bulletins/staff-accounting-bulletin-122.

[5]Custody of Digital Asset Securities by Special Purpose Broker-Dealers, 86 Fed. Reg. 11627 (Feb. 26, 2021).

[6] https://www.sec.gov/newsroom/speeches-statements/crenshaw-remarks-crypto-roundtable-tokenization-051225.

[7] https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-crypto-roundtable-tokenization-051225.

[8] https://www.sec.gov/newsroom/speeches-statements/uyeda-remarks-crypto-roundtable-tokenization-051225.

DEEPFAKES AND THE AI ARMS RACE IN BANK CYBERSECURITY

By Michael S. Barr

Michael Barr is a member of the board of governors of the Federal Reserve System. He served as Vice Chair for Supervision of the Board of Governors of the Federal Reserve System from July 2022 to February 2025. The following is edited from remarks that he gave on April 17, 2025.

Thank you for the opportunity to speak to about artificial intelligence ("AI") and cybersecurity.[1] In the past, a skilled forger could pass a bad check by replicating a person's signature. Now, advances in AI can do much more damage by replicating a person's entire identity. This technology—known as deepfakes—has the potential to supercharge identity fraud. I've recently spoken about the importance of recognizing both the benefits and the risks of generative AI ("Gen AI").[2] Today, I'd like to focus more on the darker side of the technology—specifically how Gen AI has the potential to enable deepfake technology, and what we should be doing now to defend against this risk in finance.

Escalating Threat of Gen-AI Facilitated Cybercrime

Cybercrime is on the rise, and cybercriminals are increasingly turning to Gen AI to facilitate their crimes. Criminal tactics are becoming more sophisticated and available to a broader range of criminals. Estimates of direct and indirect costs of cyber incidents range from 1 to 10% of global GDP.[3] Deepfake attacks have seen a twentyfold increase over the last three years.[4]

Cybercrime with deepfakes involves the same cat and mouse game common to sophisticated criminal activity. Both cybercriminals and financial institutions are constantly trying to outdo each other. Criminals develop new attack methods, and companies respond with better defenses. Here, the same technological innovations that enable the bad actors can also help those fighting cybercrime. However, there is an asymmetry—the fraudsters can cast a wide net of approaches and target a wide number of victims, and they only need a small number to be successful. Their marginal cost is generally low, and individual failures matter little. Conversely, companies must undergo a rigorous review and testing process to mount effective cyber defenses and will thus be slower in developing their defenses. A single failure is very costly. As we consider this issue from a policy perspective, we need to take steps to make attacks less likely by raising the cost of the attack to the cybercriminals and lowering the costs of defense to financial institutions and law enforcement.

Anatomy of a Deepfake

Deepfake attacks are those in which an attacker uses Gen AI to create a doppelganger with a person's voice or image and uses this doppelganger to interact with individuals or institutions to commit fraud. Deepfake technology is a particularly pernicious vehicle for cybercrime.[5] The process begins with voice synthesis, where Gen AI models can synthesize the speech of their victim not only in words, but also in phrase patterns, tone, and inflection. With just a short sample audio, for example, criminals assisted by Gen AI can impersonate a close relative in a crisis situation or a high-value bank client, seeking to complete a transaction at their bank.[6]

Criminals can also use Gen AI-generated videos to create believable depictions of individuals. For videos, Generative Adversarial Networks ("GANs") are the core technology behind most deepfake systems.[7] GANs consist of two competing models, the generator and the discriminator, which compete with and improve each other. This competition results in increasingly realistic, indistinguishable fake images and videos.[8]

Deepfake technology can also be augmented by other AI tools; for instance, criminals can use AI to extract and organize extensive multimodal personal data to facilitate identity verification. Attackers can also turn to "dark web" tools, such as jailbroken versions of popular large language models, where the guardrails have been removed, to learn the deepfake trade and improve their attacks.[9]

Deepfakes in Action

I expect that many of you can recall examples of how deepfakes of politicians and prominent business executives have fooled the public and spread disinformation. Deepfakes are also being used to commit payment fraud. In one case in 2024, a sophisticated deepfake of the chief financial officer for British engineering and architectural firm Arup was reportedly deployed in a video meeting and convinced an Arup financial employee to transfer $25 million to thieves.[10]

In another case, an attacker attempted to undertake a highly convincing audio deepfake of the chief executive of Ferrari, down to mimicking his southern Italian accent.[11] The recipient of the attack—another Ferrari executive—tested the caller with a personal question only the chief executive would know, which thankfully exposed the fraud.

And these institutions and individuals are not alone—a 2024 survey finds that over 10% of companies reported experiencing deepfake fraud attempts, and few steps have been taken to mitigate the risks.[12]

Particularly since COVID-19, we conduct much of our professional and personal lives over video. When we see realistic and interactive video images of a loved one in trouble, we are disposed to trust them and do what we can to help. Identity verification standards at banks often use voice detection, which may become vulnerable to Gen AI tools. If this technology becomes cheaper and more broadly available to criminals—and fraud detection technology does not keep pace—we are all vulnerable to a deepfake attack. These attacks can have significant financial costs to the victims of the crime and can also pose costs to society, eroding trust in communications and in institutions.

Defending Against Deepfakes

So what should we do? As I mentioned above, we should take steps to lessen the impact of at-

tacks by making successful breaches less likely, while making each attack more resource-intensive for the attacker.

Let me start with ways to make successful breaches less likely. A key step is to recognize the importance of strong, resilient financial institutions in preventing attacks. Banks are frontline defenders against deepfake-enabled fraud due to their direct involvement with financial transactions and customer data. To verify payors, banks maintain identity verification processes, including multi-factor authentication and account monitoring practices. To the extent deepfakes increase, bank identity verification processes should evolve in kind to include AI-powered advances such as facial recognition, voice analysis, and behavioral biometrics to detect potential deepfakes. Other techniques focus on assessing the probability that AI has been used in audio or video based on underlying metadata and then flagging the identity or transaction for further review using other verification. These technical solutions can detect subtle inconsistencies in video and audio that human observers may miss.

Banks have two points of control over the transaction—confirming not only the sender's identity, but also the legitimacy of the recipient address. They can scrutinize the recipients of large or unusual transactions, employing advanced analytics to flag suspicious patterns that could indicate fraudulent activities, and perform additional reviews before authorizing a payment to a recipient that raises flags. Banks also invest in their human controls by maintaining up-to-date training for staff on the emerging risks and incorporating the necessary security measures to mitigate the damages from breaches when they occur. And they are engaging with other financial institutions to help define the threat and identify appropriate controls and mitigants.[13]

Customers should do their part, enabling multi-factor authentication on their accounts and verifying unusual requests through a separate channel, even if the person making the request seems genuine. They should seek out education for themselves and their loved ones to help them detect and prevent fraud before it occurs.[14] And customers should value strong security practices at their financial institutions, including those which may add some friction to the user experience. The customers that may be the highest-value targets for criminals are often those with the largest digital presence, and thus most susceptible to deepfakes. They are also the customers who may prefer the most frictionless user experience, making detecting deepfakes more difficult. When it comes to protecting our money, we ought to expect and appreciate a little friction.

Regulators can help to reinforce the importance of cyber defenses in safe and sound banking through appropriate updates to guidance and regulation. As with all rules, we should be mindful of the impacts on smaller institutions and help ensure that rules are right-sized for the risk. In addition, we can work with core providers to understand the extent to which they are incorporating AI advancements in their products and services to help smaller banks defend against deepfakes and other emerging risks from the technology. Last, we can also highlight research and development for cybersecurity startups and research into tools to combat deepfakes and Gen AI-based fraud.

Regulators should consider how we could leverage AI technologies ourselves, including to enhance our ability to monitor and detect patterns of fraudulent activity at regulated institutions in real

time. This could help provide early warnings to affected institutions and broader industry participants, as well as to protect our own systems.

In addition to preventing attacks, we should also explore ways of making attacks more costly. These may include coordination with domestic and global law enforcement, internationally consistent laws against cybercrime, and continued improvement on sharing threat intelligence and insights in real-time. The official sector and banks should continue efforts to improve fraud data sharing within the financial sector and help institutions respond more quickly to emerging Gen AI-driven threats. This will make it far harder for fraudsters to operate undetected, increasing the complexity and cost of their activities. But the sharing is only as good as the data, and banks must do their part. We should help ensure that banks and other regulated institutions meet their duties to report cyber incidents in a timely way, and regulators should too.[15]

Another way to disrupt the economics of cybercrime is by increasing penalties for attempting to use Gen AI to commit fraud and increasing investment in cybercrime enforcement. This includes targeting the upstream organizations that benefit from illegal action and strengthening anti-money-laundering laws to disrupt illicit fund flows and freeze assets related to cybercrime. The fear of severe legal consequences could help to deter bad actors from pursuing AI-driven fraud schemes in the first place.

Conclusion

Deepfakes are only one of many new techniques to facilitate cyberattacks, but they feel particularly salient because they are so personal. And they are on the rise. We will need financial institutions to adapt, collaborate, and innovate in the face of these emerging threats.

ENDNOTES:

[1]The views expressed here are Barr's own and are not necessarily those of his colleagues on the Federal Reserve Board or the Federal Open Market Committee.

[2]Michael S. Barr, "Artificial Intelligence: Hypothetical Scenarios for the Future" (speech at the Council on Foreign Relations, New York, NY, February 18, 2025 (https://www.federalreserve.gov/newsevents/speech/barr20250218a.htm)); Michael S. Barr, "AI, Fintechs, and Banks" (speech at the Federal Reserve Bank of San Francisco, San Francisco, CA, April 4, 2025; https://www.federalreserve.gov/newsevents/speech/barr20250404a.htm).

[3]International Monetary Fund, Global Financial Stability Report, chapter 3 (October 2024), *See also*, World Economic Forum, Why We Need Global Rules to Crack Down on Cybercrime (January 2023; https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/).

[4]Fraud attempts with deepfakes have increased by 2137% over the last three years," Signicat, February 20, 2025, https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year#:~:text=Evolving20AI2Dbased20techniques20pose,AI2DDriven20Identity20Fraud20report.

[5]Federal Bureau of Investigation, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," public service announcement, December 3, 2024 (https://www.ic3.gov/PSA/2024/PSA241203#:~:text=AI2DGenerated20Audio2C20aka20Vocal20Cloning&text=Criminals20generate20short20audio20clips,assistance20or20demanding20a20ransom).

[6]*See* note 5.

[7]Tianxiang Shen, Ruixian Liu, Ju Bai, and Zheng Li, "Deep Fakes" Using Generative Adversarial Networks (GAN) (https://noiselab.ucsd.edu/ECE228_2018/Reports/Report16.pdf). McAfee, Beware the Artificial Impostor (May 2023), http

s://www.mcafee.com/content/dam/consumer/en-us/resources/cybersecurity/artificial-intelligence/rp-beware-the-artificial-impostor-report.pdf.

[8]"What is a GAN?" AWS, https://aws.amazon.com/what-is/gan/#:~:text=A20generative20adversarial20network20(GAN,from20a20database20of20songs.

[9] KELA, The State of Cybercrime 2025 Report (February 2025), https://www.kelacyber.com/resources/research/state-of-cybercrime-2025/.

[10]Kathleen Magramo, "British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim," CNN Business, May 17, 2024, https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html.

[11] Sandra Galletti and Massimo Pani, "How Ferrari Hit the Brakes on a Deepfake CEO," MIT Sloan Management Review, January 27, 2025 (https://sloanreview.mit.edu/article/how-ferrari-hit-the-brakes-on-a-deepfake-ceo/).

[12]Chad Brooks, "1 in 10 Executives Say Their Companies Have Already Faced Deepfake Threats," business.com, June 28, 2024, https://www.business.com/articles/deepfake-threats-study/.

[13]*See*, for instance, FS-ISAC's report on deepfake threats and risk management at https://www.fsisac.com/hubfs/Knowledge/AI/DeepfakesInTheFinancialSector-UnderstandingTheThreatsManagingTheRisks.pdf.

[14] There are a variety of public and private resources that can help. *See*, for example, the National Security Agency/Central Security Service at https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3523329/nsa-us-federal-agencies-advise-on-deepfake-threats/; and the National Cybersecurity Alliance at https://www.staysafeonline.org/articles/why-your-family-and-coworkers-need-a-safe-word-in-the-age-of-ai.

[15]Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 Fed. Reg. 66,424 (November 23, 2021) (https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank).

FINTECH LAW REPORT: APRIL-MAY 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 is a senior associate at the same firm. www.alston.com.

REGULATORY DEVELOPMENTS

President Trump Issues Executive Order to Mandate Use of Electronic Payments for Federal Government Payments

On March 25, 2025, President Trump issued an executive order, entitled "Modernizing Payments To and From America's Bank Account" ("Modernizing Payments Order").[1] The Modernizing Payments Order asserts that paper-based payments, such as checks and money orders, are susceptible to fraud, delay, and "unnecessary costs" and mandates that all Federal disbursements be made via electronic payments. The Modernizing Payments Order requires Treasury to cease issuing paper checks for Federal disbursements by September 30, 2025.

Payments to the Federal government should also be made electronically. The Modernizing Payments Order requires that payments to the government be processed electronically "as soon as practicable" and requires certain agencies to take action to terminate lockbox services and to receive payments electronically.

The Modernizing Payments Order provides some exceptions to the electronic payments

mandate. The mandate generally only applies "to the extent permissible under applicable law." There are also exceptions for individuals who do not have access to electronic payments, emergency payments, and payments related to national security or law enforcement activities. Treasury may also issue regulations or guidance providing additional exceptions.

In order to support the transition, the Modernizing Payments Order requires Treasury and the agencies to inform the public of the transition, to advise on how to access electronic payment options, and to support affected persons. Treasury must also work with industry stakeholders to address unbanked and underbanked persons.

You can access the Modernizing Payments Order here: https://www.federalregister.gov/documents/2025/03/28/2025-05522/modernizing-payments-to-and-from-americas-bank-account.

OCC and Treasury Department Announce Data Breach

On April 8, 2025, the Office of the Comptroller of the Currency ("OCC") announced that it notified Congress that it had experienced a "major" security incident.[2] This announcement came after the OCC identified suspicious activity in February between a system administrative account in its office automation system and OCC user mailboxes.[3] The OCC determined unauthorized access occurred after internal and independent third-party reviews.[4] Although internal and independent third-party reviews are still ongoing, the OCC determined that the information accessed in the breach met the conditions to classify the incident as "major."[5] Information accessed included "highly sensitive information relating to the financial condition of federally regulated financial institutions used in its examinations and supervisory oversight processes."[6] In response, the OCC is evaluating its security policies and procedures.[7]

On April 14, 2025, the OCC sent a letter to its supervised institutions regarding the incident ("Security Breach Letter").[8] According to the Security Breach Letter, the OCC continues to evaluate the content of the accessed information, make improvements to its cloud environment, and assess its security policies and procedures. The OCC also informed institutions that it will continue to share information about the incident, including advising individual institutions whether its specific information was accessed.

You can access the OCC's press release here: https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html.

You can access the Security Breach Letter here: https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32a.pdf.

CFPB Continues Efforts to Reverse Actions of Prior Administration

On March 28, 2025, the Consumer Financial Protection Bureau (the "CFPB") announced that it will not enforce various provisions of the Payday, Vehicle Title, and Certain High-Cost Installment Loans Regulation ("Payday Lending Final Rule"), including provisions relating to penalties or fines associated with the payment withdrawal provisions and the payment disclosure provisions of the rule, once they become operative on March 30, 2025.[9]

On April 11, 2025, the CFPB dropped its case against Comerica Bank, filing a notice of dismissal without prejudice.[10] The lawsuit was originally filed against Comerica Bank in December 2024 under former Director Rohit Chopra in con-

nection with Comerica's handling of the Federal Direct Express program.[11] This move follows similar dismissals of lawsuits filed under Director Chopra against Early Warning Services[12] and Capital One[13] in the last few months, although these cases were dismissed with prejudice.

On May 12, 2025, the CFPB rescinded 67 pieces of prior agency guidance ("CFPB Rescission Rule").[14] The CFPB Rescission Rule follows an April 11 memorandum from Acting Director Russell Vought ordering a review of all guidance documents and "prohibiting improper use of guidance" by the CFPB.[15] Although the guidance has been rescinded, the CFPB will evaluate "(1) whether the guidance is statutorily prescribed[;] (2) whether the interpretation therein is consistent with the relevant statute or regulation[;] and (3) whether it imposes or decreases compliance burdens."[16] Guidance may be reissued after a determination that it is necessary and reduces compliance burdens.[17] The CFPB Rescission Rule also states that the CFPB is reducing its enforcement activities in light of the president's directives to "deregulate and streamline bureaucracy," focusing only on enforcement in areas that are statutorily required and mitigating duplicative efforts of other federal and state regulators.[18]

You can access the CFPB Rescission Rule here: https://www.federalregister.gov/documents/2025/05/12/2025-08286/interpretive-rules-policy-statements-and-advisory-opinions-withdrawal.

You can access the CFPB's Payday Lending Final Rule announcement here: https://www.consumerfinance.gov/about-us/newsroom/cfpb-offers-regulatory-relief-for-small-loan-providers/.

The case before the United States District Court for the Northern District of Texas is *Consumer Financial Protection Bureau v. Comerica Bank,* Case No. 3:24-cv-03054-B. You can access the docket here: https://ecf.txnd.uscourts.gov/cgi-bin/DktRpt.pl?135362725350335-L_1_0-1.

You can access the House Financial Services Committee letter here: https://financialservices.house.gov/uploadedfiles/2025-03-28_letter_to_cfpb.pdf.

Federal Regulators Withdraw Guidance for Banks on Crypto and Digital Asset Activities

On April 24, 2025, the Board of Governors of the Federal Reserve System ("Board") announced the rescission of two supervisory letters.[19] First, the Board rescinded a 2022 supervisory letter that required state member banks to evaluate the risks and legal requirements for any planned crypto-related activities and to notify the Board before engaging in such activities. Second, the Board rescinded a 2023 supervisory letter that addressed the supervisory nonobjection process for state member banks to engage in activities related to tokens issued by distributed ledger or similar technology to facilitate payments. The Board also joined the Federal Deposit Insurance Corporation and the OCC to rescind two 2023 joint statements addressing crypto asset risks and risk management expectations.[20]

You can access the Board's announcement here: https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250424a.htm.

CFPB Withdraws Proposed Interpretive Rule Expanding Scope of Regulation E

On May 14, 2025, the CFPB issued a withdrawal of its proposed rule on the applicability of the Electronic Fund Transfer Act ("EFTA") and Regulation E to new and emerging forms of payments, fund transfers, and digital technologies

("Emerging Payments Interpretive Rule").[21] The Emerging Payments Interpretive Rule evaluated how emerging payment methods could be subject to the EFTA and Regulation E.[22] The CFPB concluded that covered entities subject to the EFTA include "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."[23] Covered "accounts" 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."[24] This could include video game accounts, virtual currency wallets, and credit card rewards points accounts.[25] In the withdrawal notice, the CFPB explained that the Emerging Payments Interpretive Rule "does not align with current agency needs, priorities, or objectives" and that the CFPB is evaluating the need for guidance on this issue.[26]

You can access the withdrawal notice here: https://public-inspection.federalregister.gov/2025-08646.pdf.

LITIGATION AND ENFORCEMENT DEVELOPMENTS

Fourth Circuit Overturns Ruling in Studco Case

On March 26, 2025, the Fourth Circuit Court of Appeals overturned a district court ruling holding that a beneficiary bank was liable to the sender under Article 4A of the Virginia Commercial Code ("VCC 4A") for ACH credits the beneficiary bank received as to which there was a name and account number mismatch ("Studco Appeal Opinion").[27] In 2018, Studco Building Systems US, LLC ("Studco"), was the victim of a business email compromise scam that resulted in Studco initiating four ACH credits to an account at 1st Advantage Federal Credit Union ("1st Advantage"), each listing Olympic Steel as the designated beneficiary. The account at 1st Advantage was held by Lesa Taylor and each transfer triggered a name mismatch alert at 1st Advantage, none of which were reviewed by 1st Advantage. The district court determined that 1st Advantage was liable to Studco because 1st Advantage would have known of the name mismatch had it implemented reasonable routines for reviewing the alerts.[28]

The Studco Appeal Opinion reversed the district court's ruling and held that 1st Advantage was not liable under VCC 4A-207(b). The court explained that, under VCC 4A-207(b), a beneficiary bank is not liable for making payment in accordance with the account number identified in the payment order when it "does not know" about a name mismatch and that "knowledge means actual knowledge, not imputed knowledge or constructive knowledge."[29] The court determined that the district court applied a constructive knowledge standard by finding that 1st Advantage would have known of the name mismatch had it exercised due diligence, even though "knowledge" is expressly defined under the VCC as "actual knowledge."[30] Further, the court found that 1st Advantage had no obligation to review the alerts because VCC 4A gives a beneficiary bank the ability to rely solely on the account number and the bank has "no duty" to identify or adopt reasonable routines to check for a name mismatch.[31] Since 1st Advantage did not have actual knowledge of the name mismatch and applied the funds in accordance with the account number stated in the payment order, the

court held that 1st Advantage was not liable for the ACH credits.[32]

The court also reversed the district court's ruling that the deposit to the account at 1st Advantage created a bailment.[33] In the Studco Appeal Opinion, the court explained that, under Virginia law, a bailment involves delivery of a chattel by the bailor, acceptance by the bailee, and an expectation that the chattel be returned to the bailor.[34] The court determined that the deposit did not create a bailment because deposits in a bank account are not chattel or goods, the deposit was not provided for a specified amount of time, and Studco did not expect to receive the deposit back from 1st Advantage.[35]

On April 9, 2025, Studco filed a petition for rehearing or rehearing en banc ("Rehearing Petition").[36] In the Rehearing Petition, Studco argues that rehearing is appropriate because (1) circumstantial evidence shows that 1st Advantage had actual knowledge of the name mismatch based on the number of times the account was reviewed during the relevant period and the other suspicious activity on the account; (2) the court considered a privity argument that 1st Advantage had forfeited; and (3) the court failed to give "significant deference" to the district court's assessment of a witness's credibility in connection with claims related to the deletion of evidence related to the alerts.[37]

On April 22, 2025, the Fourth Circuit Court of Appeals denied Studco's the Rehearing Petition.[38]

The case before the United States District Court for the Eastern District of Virginia is *Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union*, Case No. 20-cv-00417. You can access the docket here: https://ecf.vaed.uscourts.gov/cgi-bin/DktRpt.pl?483772.

Consumer Files EFTA Class Action Against Wells Fargo Related to Online Wire Transfers

On March 28, 2025, Alexandra I. Kazemier filed a putative class action complaint against Wells Fargo Bank, N.A. and Wells Fargo & Company ("Wells Fargo") related to wire transfers initiated online ("Wells Fargo Wire Complaint").[39] The plaintiff alleges that Wells Fargo failed to protect its customers from account takeover scams and to properly investigate consumer unauthorized wire transfers claims in violation of the EFTA and Article 4A of the Uniform Commercial Code ("UCC 4A"). The Wells Fargo Wire Complaint follows many of the arguments asserted by the NYAG in its case against Citi.

In the Wells Fargo Wire Complaint, the plaintiff asserts that a wire transfer initiated online by a fraudster is an unauthorized electronic fund transfer ("EFT").[40] The Wells Fargo Wire Complaint describes wire transfers in accordance with UCC 4A as consisting of a series of payment orders—(1) the sender initiates the wire transfer by "instructing [the receiving bank] to pay or cause another bank to pay the beneficiary"; (2) the receiving bank accepts the sender's payment order by "send[ing] a new payment order, either directly to the beneficiary bank . . . or through one or more intermediary banks"; and (3) the beneficiary bank "accepts the final Payment Order" and becomes obligated to pay the beneficiary.[41] The plaintiff argues that, when a fraudster gains access to a consumer's account and initiates a wire transfer, the first payment order, from the fraudster to Wells Fargo, is "to electronically authorize Wells Fargo-without consumers' knowledge or consent-to debit the consumer's account."[42] As the debits were not executed via a "service that trans-

fers funds held at either Federal Reserve banks or depository institutions," the debits are EFTs.[43]

The plaintiff asserts that Wells Fargo fails to comply with the EFTA for these unauthorized EFTs. Specifically, the plaintiff alleges that (1) Wells Fargo's agreements contractually apply UCC 4A to online consumer wire transfers, in violation of the EFTA's anti-waiver provision; (2) Wells Fargo's investigation of alleged errors involving such transfers is limited to confirming the consumer's username and password were used in connection with the transfer, in violation of the EFTA's reasonable investigation requirements; (3) Wells Fargo failed to comply with the EFTA's error resolution requirements in connection with notices of error related to online consumer wire transfers; and (4) Wells Fargo refused to reimburse amounts in excess of the EFTA's liability limits for unauthorized EFTs related to online consumer wire transfers.[44]

The Wells Fargo Wire Complaint also includes claims under UCC 4A that Wells Fargo failed to implement commercially reasonable security procedures since it relies only on a username and password for initiating online wire transfers and that Wells Fargo failed to act in good faith by accepting payment orders "in the face of anomalous activity that should have indicated suspicious or fraudulent activity."[45]

The plaintiff has requested, among other relief, actual damages, treble damages under the EFTA, attorneys' fees, costs, and interest.[46]

The case before the United States District Court for the Southern District of California is *Kazemier v. Wells Fargo Bank et al*, Case No. 3:25-cv-00727-BJC-DDL. You can access the docket here: https://ecf.casd.uscourts.gov/cgi-bin/DktRpt.pl?809417.

CFPB Drops Appeal in PayPal Case Over Prepaid Rule

On April 21, 2025, the CFPB filed a Joint Stipulation to Dismiss Appeal with PayPal, Inc. ("PayPal") to drop its appeal against a district court decision in the litigation concerning the validity of the Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z) Rule (the "Prepaid Rule"), as it applies to digital wallet products.[47] Both parties voluntarily dismissed the case with prejudice.[48]

PayPal originally filed its lawsuit against the CFPB in 2019, challenging the applicability of the Prepaid Rule to digital wallet products.[49] PayPal specifically challenged the short-form disclosure requirement, which requires providers or prepaid products to disclose specific information about fees associated with a prepaid product in a specified format.[50] *PayPal, Inc., v. Consumer Financial Protection Bureau*, No. 1:19cv3700, Doc. 48 (D.D.C. Mar. 29, 2024). The CFPB appealed this decision to the D.C. Circuit Court arguing that digital wallets and prepaid cards "share the same basic function."[52]

With the CFPB deciding to drop its appeal, the district court's ruling stands and digital wallet providers do not have to comply with the short-form disclosure requirements under the Prepaid Rule.

The case before the D.C. Circuit Court of Appeals is *PayPal, Inc., v. Consumer Financial Protection Bureau*, Case No. 24-5146. You can access the docket here: https://ecf.cadc.uscourts.gov/n/beam/servlet/TransportRoom?servlet=CaseSummary.jsp&caseNum=24-5146&incOrigDkt=Y&incDktEntries=Y and https://ecf.dcd.uscourts.

gov/cgi-bin/DktRpt.pl?caseNumber=1:19-cv-03700-RJL.

CFPB and Google Dismiss Action Related to Supervision Order

On May 8, 2025, the CFPB and Google Payment Corporation ("GPC") entered a status report in GPC's lawsuit against the CFPB to (1) notify the court that the CFPB has withdrawn its order asserting supervisory authority over GPC and (2) dismiss GPC's action ("Joint Status Report").[53] In November 2024, the CFPB issued an order designating GPC for supervision as a nonbank financial company under the Consumer Financial Protection Act in connection with GPC's Google Pay application ("GPC Supervisory Order").[54] Afterwards, GPC sued the CFPB over the GPC Supervisory Order in the U.S. District Court for the District of Columbia, arguing that the CFPB lacked a reasonable basis for exercising supervisory authority over GPC.[55] On May 7, 2025, the CFPB issued an order withdrawing the GPC Supervisory Order, stating that supervision is unwarranted because GPC has discontinued use of the Google Pay application in the U.S.[56] In the Joint Status Report, the CFPB confirmed its withdrawal of the GPC Supervisory Order and GPC dismissed its lawsuit against the CFPB without prejudice.[57]

The case before the United States District Court of the District of Columbia is *Google Payment Corporation v. Consumer Financial Protection Bureau et al.*, No. 1:24-cv-03419. You can access the docket here: https://ecf.dcd.uscourts.gov/cgi-bin/iquery.pl?124228816374389-L_1_0-1.

Citi Allowed to Appeal Court Ruling on Motion to Dismiss in NYAG EFTA Lawsuit

On April 22, 2025, the U.S. District Court for the Southern District of New York granted Citibank, N.A. ("Citi") permission to appeal ("Citi Appeal Order")[58] the court's January 21, 2025, decision ("January 2025 Order")[59] holding that consumer wire transfers initiated through online or mobile banking are not exempt from the EFTA. On February 18, 2025, Citi filed a memorandum with the court seeking leave to appeal the court's decision to the U.S. Court of Appeals for the Second Circuit and to stay the action in the district court during the appeal.[60]

In the Citi Appeal Order, the court explained that Citi had demonstrated that the EFTA interpretation it seeks to appeal involves a controlling question of law, there is substantial ground for a difference of opinion, and immediate appeal would advance the litigation.[61] The court found that the question about the EFTA's application to wire transfers is a controlling question of law that has "precedential value for a large number of cases" and the case's reversal "could significantly affect the conduct of the action."[62] The court explained that, while reversal of the decision would not terminate the litigation, it would clarify the scope of the New York Attorney General's claims and the focus of discovery.[63] The court also found that the question presents substantial ground for a difference of opinion because other courts have declined to apply the EFTA to consumer wire transfers, which shows an opposing viewpoint on the application of the EFTA.[64] Additionally, the court explained that permitting Citi's interlocutory appeal of the January 2025 Order would "materially advance" the litigation's termination and remove legal uncertainty over the proceedings since the appeal will determine whether the EFTA or Article 4A of the Uniform Commercial Code will govern the action.[65]

In the Citi appeal Order, the court stayed the

January 2025 Order, pending Citi's appeal. Although the court stated that it does not expect Citi will win on appeal, the court was persuaded by Citi's arguments regarding how the application of the EFTA to consumer wire transfers will impact the financial services industry.[66] The court also pointed out that the stay will serve public interests since it creates an opportunity to make a more binding statement on the legal standard for online consumer wire transfers.[67]

The case before the United States District Court for the Southern District of New York is *The People of the State of New York v. Citibank, N.A.*, Case No. 1:24-cv-00659-JPO. You can access the docket here: https://ecf.nysd.uscourts.gov/cgi-bin/DktRpt.pl?105544353003701-L_1_0-1.

Court Rules on Bank of America's Motion to Dismiss EFTA Lawsuit

On May 7, 2025, the U.S. District Court for the District of South Carolina held that an individual plaintiff, Robert Wailing, could proceed with his claims against Bank of America, N.A. ("BANA") alleging that the EFTA applies to wire transfers initiated by consumers through online or mobile banking.[68] Wailing alleged that BANA failed to properly investigate and reimburse unauthorized wire transfers in accordance with the EFTA and that the transfers are covered by the EFTA because they were initiated electronically through BANA's online banking platform or mobile application and the funds were first moved to the bank's account before being transmitted over a wire network to another bank.[69] In response, BANA asserted that the EFTA does not apply to the transfers at issue because wire transfers are excluded from the definition of an electronic fund transfer under the EFTA.[70]

In denying BANA's motion to dismiss, the court relied heavily on the reasoning of the District Court for the Southern District of New York in the New York Attorney General's case against Citibank ("Citi Opinion").[71] The court was persuaded by the reasoning in the Citi Opinion adopting the New York Attorney General's argument that each consumer wire transfer consists of three distinct parts: (1) the consumer's transfer of funds to the originating bank; (2) the originating bank's transfer of funds to the beneficiary bank through a wire transfer system; and (3) the beneficiary bank's transfer of funds to the beneficiary.[72] The BANA court also largely wholesale adopted the Citi Opinion's interpretation of the statutory text of the EFTA and dismissal of case law promoted by Citibank and BANA.[73] Ultimately, the BANA court concurred with the Citi Opinion that the EFTA's wire transfer exclusion "does not apply to electronic transfers of funds between consumers and their financial institutions, even when made ancillary to an interbank wire" because such transfers do not satisfy the elements of the wire transfer exclusion.[74]

The BANA court dismissed the two other claims brought by the plaintiff alleging that: (1) BANA participated in the exploitation of a vulnerable adult for not detecting and stopping the alleged unauthorized transactions because the plaintiff failed to allege a plausible claim and (2) BANA failed to comply with UCC 4A because the transfers at issue are covered by the EFTA and therefore excluded from the scope of UCC 4A.[75]

The case before the United States District Court for the District of South Carolina is *Wailing v. BANA, N.A.*, No. 8:24-cv-05223-BHH. You can access the docket here: https://ecf.scd.uscourts.gov/cgi-bin/iquery.pl?75375706624104-L_1_0-1.

Parties Move for Summary Judgement in Illinois Interchange Fee Litigation; Senator Durbin Defends State Law

On March 17, 2025, Plaintiffs filed a motion for summary judgment and permanent injunction to prohibit the Illinois Attorney General ("Illinois AG") from enforcing the Illinois Interchange Fee Prohibition Act (the "Illinois IFPA") against (1) national and out-of-state banks; (2) federal and out-of-state saving associations; (3) federal and out-of-state credit unions; and (4) other entities participating in electronic payment transactions (e.g., card networks and processors) in relation to the foregoing financial institutions.[76]

The District Court for the Northern District of Illinois initially granted a preliminary injunction against the Illinois IFPA as it applies to national banks because the National Bank Act ("NBA") preempts state laws that prevent or significantly interfere with a national bank's power to engage in the business of banking.[77] The court also extended the preliminary injunction to federal savings associations and out-of-state banks, finding that the Illinois IFPA was likely preempted by the Home Owner's Loan Act and the Riegle-Neal Interstate Banking and Branching Efficiency Act, respectively.[78] The court declined to extend the preliminary injunction to federal credit unions, as it could not conclude that the Illinois IFPA was likely preempted under the Federal Credit Union Act, and to other entities (like card networks and processors) involved in processing credit and debit card transactions on grounds that the Dodd-Frank Wall Street Reform and Consumer Protection Act expressly prohibits extending preemption to such entities.[79]

In its motion for summary judgment and permanent injunction, Plaintiffs argue that preemption must extend to "other participants in the intricately interconnected payment system" because preventing such participants from performing functions necessary to national banks' exercise of their federally granted powers would be a significant interference.[80] The Illinois AG filed a combined opposition to Plaintiffs' motion and cross motion for summary judgment on April 23, 2025.[81] The Illinois AG argues that the Illinois IFPA does not significantly interfere with national banks' powers and that preemption under the NBA does not extend to entities that are not national banks.[82]

Notably, Senator Richard Durbin (D-IL) filed an amicus brief on the same day in support of the Illinois IFPA.[83] Senator Durbin argues in his brief that, contrary to Plaintiffs' contention that the IFPA's interchange fee prohibition conflicts with and is preempted by the Durbin Amendment to the EFTA, "[t]he IFPA fully aligns with the Durbin Amendment's text, its structure, and its goal of constraining network-fixed debit interchange fees to reduce excessively high fee rates."[84] Senator Durbin further argues that because interchange fees are set by the card networks and not banks, the IFPA's regulation of interchange fees does not interfere with national banks' authority to set their own pricing.[85]

On May 7, the Plaintiffs filed a reply brief in support of their motion for summary judgement and in opposition to the Illinois AG's summary judgment motion.[86] In their reply, the Plaintiffs assert that Illinois is attempting to improperly circumvent NBA preemption by "regulating those who transact with national banks instead of the banks themselves."[87] Plaintiff contend that the only way to provide meaningful relief from this indirect interference is to issue a broad injunction

that includes the third parties on which national banks rely to exercise their federal powers.[88]

Notably, two bills have been introduced in the Illinois legislature to repeal the Illinois IFPA.[89] Both bills remain in legislative committees. The Illinois legislature adjourns on May 31 and reconvenes in the fall for two weeks to consider the Governor's vetoes.[90] The legislature reconvenes in January for the next legislative session. The Illinois IFPA becomes effective July 1, 2025.

The case before the U.S. District Court for the Northern District of Illinois is *Illinois Bankers Association v. Kwame Raoul*, Case No. 1:24-cv-07307. You can access the docket here: https://ecf.ilnd.uscourts.gov/cgi-bin/DktRpt.pl?463030.

You can access HB 1822 here: https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=114&GA=104&DocTypeId=HB&DocNum=1822&GAID=18&LegId=&SpecSess=&Session=.

You can access SB 1798 here: https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=114&GA=104&DocTypeId=SB&DocNum=1798&GAID=18&LegId=160947&SpecSess=0&Session=0.

ENDNOTES:

[1]Executive Order, *Modernizing Payment To and From America's Bank Account*, 90 Fed. Reg. 14001 (Mar. 28, 2025), https://www.federalregister.gov/documents/2025/03/28/2025-05522/modernizing-payments-to-and-from-americas-bank-account.

[2]Office of the Comptroller of the Currency, *News Release 2025-30*, Apr. 8, 2025 , https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html.

[3]*Id.*

[4]*Id.*

[5]*Id.*

[6]*Id.*

[7]*Id.*

[8]Office of the Comptroller of the Currency, *News Release 2025-32*, Apr. 15, 2025, https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32.html.

[9]*CFPB Offers Regulatory Relief for Small Loan Providers*, CFPB (Mar. 28, 2025), https://www.consumerfinance.gov/about-us/newsroom/cfpb-offers-regulatory-relief-for-small-loan-providers/.

[10]*Consumer Financial Protection Bureau. Comerica Bank*, No. 3:24-cv-03054-B, Doc. 42 (N.D. Tex. Apr. 11, 2025).

[11]*Consumer Financial Protection Bureau. Comerica Bank*, No. 3:24-cv-03054-B, Doc. 1 (N.D. Tex. Dec. 6, 2024).

[12]*Consumer Financial Protection Bureau. Early Warning Services, LLC*, No. 2:24-cv-03652-SMB, Doc. 39 (D. Ariz. Mar. 4, 2025).

[13]*Consumer Financial Protection Bureau. Capital One Financial Corp. & Capital One, N.A.*, No. 1:25-cv-00061-DJN-WBP, Doc. 20 (E.D.VA. Feb. 27, 2025).

[14]CFPB, *Withdrawal of Bureau guidance, interpretive rules, policy statements, and advisory opinions*, 90 Fed. Reg. 20,084 (May 12, 2025), https://www.federalregister.gov/documents/2025/05/12/2025-08286/interpretive-rules-policy-statements-and-advisory-opinions-withdrawal.

[15]*Id.* at 20,085.

[16]*Id.*

[17]*Id.*

[18]*Id.*

[19]*Federal Reserve Board announces the withdrawal of guidance for banks related to their crypto-asset and dollar token activities and related changes to its expectations for these activities*, Board (Apr. 24, 2025), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250424a.htm.

[20]*Id.*

[21]CFPB, *Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment Mechanisms; Withdrawal* (May 14, 2025), https://public-inspection.federalregister.gov/2025-08646.pdf.

[22]CFPB, *Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment 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.

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

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

[25]*Id*.

[26]CFPB, *Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment Mechanisms; Withdrawal* (May 14, 2025), https://public-inspection.federalregister.gov/2025-08646.pdf.

[27]*Studco Building Systems US, LLC v 1st Advantage Federal Credit Union*, No. 20-cv-00417, Doc. 167 (4th Cir. Apr. 2, 2025).

[28]*Studco Building Systems US, LLC v" 1"t Advantage Federal Credit Union*, No. 20-cv-00417, Doc. 119 (E.D.VA. Jan. 12, 2023), https://ecf.vaed.uscourts.gov/cgi-bin/DktRpt.pl?483772.

[29]Studco Appeal Opinion, *supra* note 27 at 13-14.

[30]*Id*. at 17.

[31]*Id*. at 16-17.

[32]*Id*. at 17-18.

[33]*Id*. at 18-19.

[34]*Id*.

[35]*Id*.

[36]*Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union*, No. 23-1148, Doc. 4 (4th Cir. Apr. 9, 2025).

[37]*Id*. at 12-15.

[38]*Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union*, No. 20-cv-00417, Doc. 169 (4th Cir. Apr. 22, 2025).

[39]*Kazemier v. Wells Fargo Bank et al*, No. 3:25-cv-00727-BJC-DDL, Doc. 1 (S.D.CA. Mar. 28, 2025).

[40]*Id*. at 14.

[41]*Id*. at 11.

[42]*Id*. at 13-14.

[43]*Id*. at 26.

[44]*Id*. at 18-19, 27.

[45]*Id*. at 29-30.

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

[47]*PayPal, Inc., v. Consumer Financial Protection Bureau*, No. 24-5146, Doc. 2112006 (D.C. Cir. Apr. 21, 2025).

[48]*Id*.

[49]*PayPal, Inc., v. Consumer Financial Protection Bureau*, No. 1:19cv3700, Doc. 1 (D.D.C. Dec. 11, 2019).

[50]*See* 12 C.F.R. 1006.18(b).

[52]*PayPal, Inc., v. Consumer Financial Protection Bureau*, No. 24-5146, Doc. 2081990 (D.C. Cir. Oct. 25, 2024).

[53]*Google Payment Corporation v. Consumer Financial Protection Bureau et al*., No. 1:24-cv-03419, Doc. 17 (D.D.C. May 8, 2025).

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

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

[56]*Google Payment Corporation v. Consumer Financial Protection Bureau et al*., No. 1:24-cv-03419, Doc. 17-1 (D.D.C. May 8, 2025).

[57]Joint Status Report *supra* note 53.

[58]*The People of the State of New York v. Citibank, N.A.*, No. 1:24-cv-00659-JPO, Doc. 73 (S.D.N.Y. Apr. 22, 2025).

[59]*The People of the State of New York v. Citibank, N.A.*, No. 1:24-cv-00659-JPO, Doc. 49 (S.D.N.Y Jan. 21, 2025).

[60]*The People of the State of New York v. Citibank, N.A.*, No. 1:24-cv-00659-JPO, Doc. 55 (S.D.N.Y. Feb. 18, 2025).

[61]Citi Appeal Order, *supra* note 58.

[62]*Id*. at 5.

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

[64]*Id*. at 7-8.

[65]*Id*. at 8-9.

[66]*Id*. at 10.

[67]*Id*. at 11.

[68]*Wailing v. Bank of America, N.A.*, No. 8:24-cv-05223-BHH. Doc. 43 (D.S.C. May 8, 2025).

[69]*Id*. at 3-4.

[70]15 U.S.C.A. § 1693a(7)(B).

[71]*Wailing v. Bank of America, N.A.*, No. 8:24-cv-05223-BHH. Doc. 43. at 5-13 (D.S.C. May 8, 2025). *See The People of the State of New York v. Citibank, N.A.*, No. 1:24-cv-00659, Doc. 49 (S.D.N.Y Jan. 21, 2025).

[72]*Wailing v. Bank of America, N.A.*, No. 8:24-cv-05223-BHH. Doc. 43 at 7-8 (D.S.C. May 8, 2025).

[73]*Id*. at 8-11.

[74]*Id*. at 12.

[75]*Id*. at 13-17.

[76]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Docs. 123, 125 (N.D. Ill. Mar. 17, 2025).

[77]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 120 (N.D. Ill. Dec. 20, 2024).

[78]*Id*.; *Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 115 (N.D. Ill. Feb. 6, 2025).

[79]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 115 at 7 (N.D. Ill. Feb. 6, 2025).

[80]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 125 at 33 (N.D. Ill. Mar. 17, 2025).

[81]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 138 (N.D. Ill. Apr. 23, 2025).

[82]*Id*.

[83]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 139 (N.D. Ill. Apr. 23, 2025).

[84]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 139 at 5 (N.D. Ill. Apr. 23, 2025).

[85]*Id*. at 5-12.

[86]*Illinois Bankers Association v. Kwame Raoul*, No. 1:24-cv-07307, Doc. 146 (N.D. Ill. May 7, 2025).

[87]*Id*. at 3, 7-9.

[88]*Id*. at 28-30.

[89]Senate Bill No. 1798, Illinois General Assembly (Feb. Session, 2025), https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=114&GA=104&DocTypeId=SB&DocNum=1798&GAID=18&LegID=160947&SpecSess=0&Session=0; House Bill No. 1822, Illinois General Assembly (Jan. Session, 2025), https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=114&GA=104&DocTypeId=HB&DocNum=1822&GAID=18&LegId=&SpecSess=&Session=.

[90]*Legislative Days for Calendar Year 2025*, Illinois House of Representatives, https://www.ilga.gov/house/schedules/legis_days_2025.pdf (last visited May 14, 2025).

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.