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

July/August 2023 ▪ Volume 26 ▪ Issue 4

SEC V. RIPPLE LABS, INC., ET AL.: A TURNING POINT IN CRYPTOCURRENCY JURISPRUDENCE?

By David I. Miller and Charles J. Berk

David Miller is a Shareholder at Greenberg Traurig, LLP and a former Assistant US Attorney for the Southern District of New York. Charles Berk is an associate at the firm. Contact: david.miller@gtlaw.com or berkc@gtlaw.com.

On July 13, 2023, in a highly anticipated decision for the cryptocurrency industry, a Southern District of New York court granted in part and denied in part the parties' cross motions for summary judgment in *SEC v. Ripple Labs, Inc., et al.*[1] Despite mixed rulings, the decision has been viewed by several in the cryptocurrency community as a victory for Ripple Labs, Inc. and the individual co-defendants (collectively, "Ripple"), and for cryptocurrency enterprises more broadly. In its summary judgment filings, the Securities and Exchange Commission alleged that Ripple engaged in three categories of unregistered XRP token offers and sales in violation of Section 5 of the Securities Act of 1933: (1) "Institutional Sales" under written contracts for which it received $728 million; (2) "Programmatic Sales" on digital asset exchanges for which it received $757 million; and (3) "Other Distributions" under written contracts for which it recorded $609 million in "consideration other than cash." While the Court agreed with the SEC that Ripple's Institutional Sales were unregistered securities transactions, Judge Analisa Torres found to the contrary regarding Ripple's Programmatic Sales and Other Distributions. The Court's decision regarding these two transaction categories—that they were not "investment contracts" and thus not securities—constitutes a notable departure from

IN THIS ISSUE:

THOMSON REUTERS®

42972644

other recent SEC cryptocurrency cases[2] in which the SEC secured victories in its ongoing cryptocurrency enforcement campaign.

BACKGROUND

Ripple Labs, Inc. is a technology company founded in 2012 that has developed the Ripple payment protocol and exchange network. Ripple offers an open-source payment system and a digital currency token, XRP, that allows for currency exchange, payment, and money transfers on Ripple's blockchain, which is known as the XRP Ledger. A "blockchain" is a cryptographically secured ledger that tracks the current and historical state of accounts, transactions, and/or events occurring on a network of computers, and is maintained by multiple parties, often referred to as validators or miners—who validate transactions occurring among users on the network. Transactions are grouped together over some time interval and posted to the ledger in "blocks," and each block is cryptographically linked to the previous block, creating an unbroken chain of valid transactions. As alleged in the SEC's Amended Complaint (filed in February 2021), from at least 2013 through February 2021, Ripple engaged in securities transactions involving over 14.6 billion units of XRP worth over $1.38 billion but failed to register those sales with the SEC as would be required by the securities laws if the relevant offerings were, in fact, investment contracts.

The question before the court was whether Ripple's offers and sales of the XRP token were "investment contracts" and thus transactions in a security requiring registration with the SEC. While not defined by statute, the U.S. Supreme Court in *SEC v. W.J. Howey Co.*[3] provides the seminal analysis for what constitutes an "investment contract" and thus a security under Section 5. Specifically, the Supreme Court held that under the Securities Act, an investment contract is "a contract, transaction[,] or scheme whereby a person [(1)] invests his money [(2)] in a common enterprise and [(3)] is led to expect profits solely from the efforts of the promoter or a third party."[4]

THE PARTIES' ARGUMENTS

In September 2022, following substantial discovery, the SEC and Ripple each filed mo-

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

One Year Subscription ● 6 Issues ● $ 1020.00

tions for summary judgment. The SEC's filings urged that as a matter of economic reality, purchases of XRP are "investment contracts" satisfying all three prongs of the *Howey* test. The SEC claimed that XRP purchasers invested their money in a "common enterprise" under *Howey*, arguing that all of Ripple's offerings and sales exhibited both horizontal and strict vertical commonality. The SEC claimed horizontal commonality, which "ties the fortunes of each investor in a pool of investors to the success of the overall venture," was present because XRP tokens are all fungible, and because XRP's market price increases or decreases for all units of XRP "together and equally."[5] And notably, the SEC asked the Court to echo Judge Alvin K. Hellerstein's finding in *SEC v. Kik Interactive, Inc.* that "[t]he economic reality is that" the defendant "pooled proceeds from its sale" of its digital token "in an effort to boost the value of the investment," such that "[t]he stronger the ecosystem that" the defendant "built, the greater the demand for" the digital token "and thus the greater the value of each purchaser's investment."[6]

The SEC also argued that even absent horizontal commonality, the Court could find strict vertical commonality (which requires that "the fortunes of investors be tied to the fortunes of the promoter") because, as a matter of economic reality, Ripple's ownership of and dependence on selling XRP to fund its operations proved that the success or failure of the token would affect the fortunes of Ripple, its executives, and XRP investors.[7] Rounding out its *Howey* analysis, the SEC contended that XRP's purchasers reasonably expected to profit from their XRP purchases because Ripple marketed and promoted XRP as an investment. In support, the SEC cited a wide range of Ripple's statements, including informational brochures, internal talking points, public blog posts, statements on social media, videos, interviews with various Ripple employees, and more.[8] Lastly, the SEC alleged that the individual defendants—Ripple executives Bradley Garlinghouse and Christian Larsen—aided and abetted Ripple's purported violations of the securities laws, and urged the Court to reject the defendants' due process defenses.[9]

In contrast, Ripple's summary judgment motion (and its opposition to the SEC's motion) argued that Ripple's offers and sales of XRP lacked the "essential ingredients" of an investment contract.[10] The defense urged the Court to look to the so-called "blue sky" law cases on which *Howey* relied to find that all investment contracts must contain the following "essential ingredients": (1) a contract between a promoter and an investor that establishes the investor's rights as to an investment; (2) the contract imposes post-sale obligations on the promoter to take specific actions for the investor's benefit; and (3) the contract grants the investor a right to share in profits from the promoter's efforts to generate a return on the use of investor funds.[11] Ripple claimed that the "essential ingredients" test "give[s] meaning and structure to the *Howey* test," and argued that the SEC's inability to show the presence of these "ingredients" was fatal to its claims.[12]

Turning to the elements of the *Howey* test itself, Ripple stated that in many of the transactions at issue, those who received XRP from Ripple did not provide any consideration and,

accordingly, no "investment of money" occurred.[13] Moreover, Ripple maintained that even for sales of XRP in which a buyer did pay money to Ripple (rather than receiving XRP as a form of compensation), the SEC still could not satisfy the first *Howey* element because *Howey* requires an *investment* of money, as opposed to a mere *payment* of money: "If mere payment were sufficient to satisfy the first *Howey* element, then that element would have no meaningful effect; it would be satisfied not just for people buying investment contracts in orange groves, but for people who bought oranges at the supermarket."[14]

Ripple further argued that, contrary to the SEC's contention, no "common enterprise" existed among holders of the XRP token. Ripple urged that XRP's fungible nature does not suggest the existence of a "common enterprise" and instead argued that XRP should be compared to gold or other fungible assets that are not traditionally considered securities: "That XRP is fungible does not mean that XRP holders depend upon one another to earn profits; it means that those who own XRP as an investment have a common interest in XRP's price when they decide to sell . . . it could just as well be said that all owners of gold share a common interest in the price of gold; or that all owners of soybeans or of pigs share a common interest in the price of soy or pork. Those owners are still not engaged in a common enterprise because they do not depend upon one another to earn profits on sales."[15] Ripple went on to argue that the SEC could show neither horizontal nor strict vertical commonality, explaining that XRP holders have no participatory interest in any common "pool" of assets and that the fortunes of Ripple and XRP holders were not inextricably linked.[16] In other words, Ripple claimed, XRP holders might experience losses while Ripple maintained positive income, and vice versa.[17] Ripple also contended that XRP holders' profits were not due to the "efforts of the promoter" as required by *Howey*, but instead were primarily a result of market forces.[18] Additionally, Ripple argued that it never made any promises or statements to purchasers sufficient to create a reasonable "expectation of profits" as required by *Howey*.[19] Finally, Ripple propounded fair notice and due process arguments for why the SEC was not entitled to summary judgment. The Court addressed the parties' arguments in a comprehensive 34-page opinion.

THE COURT'S DECISION

RELEVANT BACKGROUND AND LEGAL STANDARDS

The Court began its opinion by outlining the critical facts underpinning its analysis. First, the Court walked through the SEC's allegation that Ripple conducted three categories of improper XRP offerings without filing any registration statements, financial statements, or other periodic reports with the SEC: (1) "Institutional Sales" through which Ripple sold XRP directly to institutional buyers, hedge funds, and other sophisticated customers pursuant to written contracts; (2) "Programmatic Sales" or blind transactions through the use of trading algorithms made on digital asset exchanges; and (3) "Other Distributions" through which Ripple distributed XRP as a form of payment for services (*e.g.*, XRP distributions made to Ripple employees as a form of compensation).[20] The

Court also noted that in addition to Ripple's sales and offers, co-defendants Garlinghouse and Larsen offered and sold XRP in their individual capacities during the relevant period.[21] In embarking on its analysis, the Court observed that Ripple represented to the public that it would search for "use" and "value" for XRP, and that Ripple received legal advice to the effect that "[t]he more that [the founders and Ripple] promote [XRP] as an investment opportunity, the more likely it is that the SEC will take action and argue that [XRP tokens] are 'investment contracts.' "[22]

Next, Judge Torres briefly laid out the relevant legal standards concerning Section 5 and the *Howey* test.[23] The Court then discussed—but swiftly rejected—Ripple's proposed "essential ingredients" test, concluding that two of the "essential ingredients" advocated by Ripple fall outside the scope of *Howey*'s requirements.[24] The Court ruled that *Howey*'s focus is on a purchaser's expectation of "profits . . . from the efforts of others," emphasizing that the test is intended to "embod[y] a flexible rather than a static principle," thus rejecting the "essential ingredients" test's more rigid requirements that investment contracts impose formal post-sale obligations on a promoter and/or provide a formal grant to an investor of a right to share in profits.[25] Critically, though, the Court declined to evaluate the merits of the first "essential ingredient," *i.e.*, whether an "investment contract" under *Howey* presumes the existence of an *underlying contract* between the parties. According to the Court, such an analysis was not necessary here, as "in each instance where Defendants offered or sold XRP as an investment contract, a contract existed."[26]

Consistent with *Telegram, Kik*, and *LBRY*, the Court clarified that whether Ripple's XRP offerings constitute investment contracts must turn on the totality of the circumstances surrounding each transaction, rather than just on the inherent character or nature of an underlying asset. The Court explained, "if the original citrus groves in *Howey* were later resold, those resales may or may not constitute investment contracts, depending on the totality of circumstances surrounding the later transaction."[27] Thus, the Court reasoned, Ripple's suggestion that XRP itself, like gold or other "ordinary assets," cannot be a security, "misses the point because ordinary assets—like gold, silver, and sugar—may be sold as investment contracts, depending on the circumstances of those sales."[28]

RIPPLE'S XRP OFFERINGS AND SALES

The Court then turned its attention to the first relevant category of XRP offerings, namely Ripple's Institutional Sales of XRP (made pursuant to written contracts). In deeming Ripple's Institutional Sales "investment contracts," the Court was unpersuaded by the defense's argument that *Howey*'s first element—requiring an investment of money—was not satisfied. Specifically, the Court rejected Ripple's view that an "investment of money" is different from "merely payment of money," and instead held that simply "provid[ing] [] capital" is sufficient to establish *Howey*'s first element.[29]

The Court also found horizontal commonality with regard to the Institutional Sales, noting that "each Institutional Buyer's ability to profit

was tied to Ripple's fortunes and the fortunes of other Institutional Buyers because all Institutional Buyers received the same fungible XRP. Ripple used the funds it received from its Institutional Sales to promote and increase the value of XRP by developing uses for XRP and protecting the XRP trading market. When the value of XRP rose, all Institutional Buyers profited in proportion to their XRP holdings."[30] Accordingly, the Court determined that as to the Institutional Sales, *Howey*'s "common enterprise" element was satisfied.[31]

As for *Howey*'s third element—whether Ripple's institutional purchasers had "a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others"—the Court again sided with the SEC, citing numerous examples of Ripple's statements and marketing materials linking Ripple's efforts with XRP's value.[32] The Court added that Ripple's transactions with the institutional purchasers—which were typically highly sophisticated entities such as hedge funds—included sales contracts with limitations such as lockup provisions and resale restrictions, supporting the conclusion that the Institutional Sales were sold as investments rather than for consumptive use.[33] And in so ruling, Judge Torres echoed the Court's language in *SEC v. LBRY, Inc*., finding that an expectation of profits "need not be the sole reason a purchaser buys an investment; an asset may be sold for both consumptive and speculative uses."[34] Having found that all three *Howey* elements were satisfied, the Court held that Ripple's Institutional Sales were "investment contracts" that ran afoul of the U.S. securities laws.

Though the Court sided with the SEC as to the Institutional Sales, importantly, it found in favor of Ripple regarding its Programmatic Sales of the XRP token. The Court began this portion of its analysis by jumping immediately into *Howey*'s third element, noting that purchasers of Ripple's Programmatic Sales participated in blind transactions, unable to know whether their payments were being sent to Ripple or elsewhere. The Court contrasted the Programmatic Sales with Ripple's Institutional Sales: "[w]hereas the Institutional Buyers reasonably expected that Ripple would use the capital it received from its sales to improve the XRP ecosystem and thereby increase the price of XRP, Programmatic Buyers could not reasonably expect the same. Indeed, Ripple's Programmatic Sales were blind bid/ask transactions, and Programmatic Buyers could not have known if their payments of money went to Ripple, or any other seller of XRP."[35] The Court added, "[i]t may certainly be the case that many Programmatic Buyers purchased XRP with an expectation of profit, but they did not derive that expectation from Ripple's efforts (as opposed to other factors, such as general cryptocurrency market trends)—particularly because none of the Programmatic Buyers were aware that they were buying XRP from Ripple."[36] The Court's holding in this regard appears to support similar arguments defense counsel recently advanced in *SEC v. Wahi*, contending that token transactions executed on a digital asset exchange do not satisfy *Howey* because in addition to there being no contract between the issuer/promoter and the purchaser, the purchaser's expectation of profits is derived primarily from market forces rather than from manage-

rial efforts emanating from a contract.[37] Critically, however, the Court in *Ripple* declined to address directly whether secondary market sales of XRP constitute an offer or sale of an investment contract.[38]

Next, the Court turned to Ripple's "Other Distributions" of XRP. Here, the Court again ruled in favor of Ripple because the "Other Distributions" did not satisfy *Howey*'s first requirement that there be an "investment of money" as part of a transaction. Simply, the Court observed that the record was clear: "recipients of the Other Distributions did not pay money or 'some tangible and definable consideration' to Ripple."[39]

Finally, the Court opined on Ripple's due process arguments. The Court rejected the fair notice and vagueness defenses as to the Institutional Sales, holding that *Howey* sets forth a clear test for determining what constitutes an investment contract, and finding that *Howey*'s progeny provides guidance as to how to apply that test to a variety of factual scenarios.[40] The Court also declined to award summary judgment on the SEC's claim that the individual defendants aided and abetted a securities violation in violation of 15 U.S.C.A. § 77o(b), concluding that the defendants "raised a genuine dispute of material fact as to whether Larsen and Garlinghouse knew or recklessly disregarded the facts that made Ripple's scheme illegal."[41]

IMPLICATIONS

Although Judge Torres' ruling granted relief to both sides, the Court's decision has been viewed as a victory for Ripple by several members of the cryptocurrency community, especially when compared to the victories secured by the SEC in other recent cases. There are several key takeaways from the Court's decision:

1. Judge Torres made clear that the relevant inquiry under *Howey* is not whether a particular asset is, in and of itself, determined to be a security, but instead whether the circumstances of the asset's offer or sale render it an investment contract and thus a security. To conduct this analysis, Courts must examine the totality of the circumstances surrounding each relevant asset transaction in a case rather than simply analyzing the character of the asset itself.

2. As we have seen in prior cases like *Telegram, Kik*, and *LBRY*, the Court in *Ripple* continued to support a pragmatic approach to *Howey*, favoring an observance of the "economic realities" behind cryptocurrency offerings in lieu of "unrealistic and irrelevant formulae."[42]

3. The Court declined to adopt the "essential ingredients" test as promulgated by the defendants. But significantly, the Court declined to opine as to the merit of the first element of that test; namely, whether the existence of an "investment contract" requires the presence of an underlying contract between two parties (be it written, oral, or implied)—because a written contract existed for the Institutional Sales.

4. The critical distinction drawn by the Court between Ripple's Institutional Sales and

its Programmatic Sales was that institutional purchasers, which were generally highly sophisticated professional entities in a written contractual relationship with Ripple, reasonably expected the funds they provided to Ripple would be used to increase XRP's value. Going forward, cryptocurrency issuers should be mindful of this distinction and carefully consider how their token sales and/or offerings are structured and presented to potential purchasers.

In sum, the *Ripple* decision is important precedent in an uncertain and developing cryptocurrency enforcement space. If not modified on appeal, *Ripple* may have significant utility for—and be used in litigation against the SEC by—cryptocurrency exchanges and secondary market purchasers who have no agreement, knowledge, or expectation that an issuer or promoter will undertake efforts to enhance token profits. Indeed, certain cryptocurrency businesses currently in litigation with the SEC over whether they are operating as unregistered securities exchanges may point to the *Ripple* decision to substantiate their belief that tokens trading in the secondary markets are not securities (even if that question was unresolved by *Ripple*). Regardless, the *Ripple* opinion appears to draw a critical distinction between direct contractual efforts between issuers/promoters and purchasers and market purchasing in the token space, and thus this decision could be the first major chink in the SEC's armor in its cryptocurrency enforcement efforts.

ENDNOTES:

[1]Unless otherwise indicated, all docket citations herein refer to the docket in *Securities and Exchange Commission v. Ripple Labs, Inc. et al.*, 20-cv-10832-AT-SN (S.D.N.Y. Dec. 22, 2020).

[2]*See* our articles on *SEC v. LBRY, Inc.* (https://www.gtlaw.com/en/insights/2022/11/sec-v-lbry-inc-the-secs-latest-crypto-victory), *SEC v. Kik Interactive Inc.* (https://www.gtlaw.com/en/insights/2020/10/another-significant-cryptocurrency-decision-sec-v-kik-interactive-inc-and-token-offerings-under) and *SEC v. Telegram Group* (https://www.gtlaw.com/en/insights/2020/4/sec-v-telegram—a-groundbreaking-decision-in-cryptocurrency-enforcement). *SEC v. Ripple* is notably distinct from *Telegram* and *Kik* in that those cases arose in the context of Initial Coin Offerings ("ICOs") or Simple Agreements for Future Tokens ("SAFT"). No such offerings are alleged here.

[3]*S.E.C. v. W.J. Howey Co.*, 328 U.S. 293, 66 S. Ct. 1100, 90 L. Ed. 1244, 163 A.L.R. 1043 (1946).

[4]*Howey*, 328 U.S. at 298-99.

[5]*See* ECF No. 837, SEC Motion for Summary Judgment ("SEC MSJ") at 50-51.

[6]*See id*. at 51.

[7]*See id.* at 52.

[8]*See id.* at 53-58

[9]*See id.* at 66-75.

[10]*See* ECF No. 825, Defendants' Motion for Summary Judgment ("Def. MSJ") at 13.

[11]*See id*. at 18-21.

[12]*Id.* at 25.

[13]*See id.* at 36-37.

[14]ECF No. 828, Defendants' Opposition to SEC's Summary Judgment Motion at 19.

[15]Def. MSJ at 43.

[16]*See id.* at 45.

[17]*See id.* at 48-49.

[18]*See id.* at 49-54.

[19]*See id.* at 50-58.

[20]*See* ECF No. 874, Summary Judgment Decision ("MSJ Decision") at 4-5.

[21]*See id.* at 5.

[22]*See id.* at 8.

[23]*See id.* at 10-11.

[24]*See id.* at 11-13.

[25]*See id*. at 12-13.

[26]*Id.* at 13.

[27]*Id.* at 14.

[28]*Id*.

[29]*Id.* at 16.

[30]*Id.* at 17-18 (internal citations omitted).

[31]After finding that horizontal commonality established the existence of a common enterprise, the Court declined to address the issue of strict vertical commonality. *Id.* at 17 n. 12.

[32]*See id.* at 19-22.

[33]*See id*. at 21.

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

[35]*Id.* at 23.

[36]*Id.* at 24. The Court dispensed with the issue of Garlinghouse and Larsen's personal sales of XRP in similar fashion. As with Ripple's Programmatic Sales, the Court held that individual defendants' XRP sales were programmatic sales on various digital asset exchanges made through blind bid/ask transactions. Thus, as a matter of law, the record did not establish the third *Howey* prong as to these transactions. *See id.* at 27-28.

[37]*See SEC v. Wahi*, 22-cv-1009-TL (W.D.Wa Feb. 6, 2023), ECF No. 33 at 52-54. The defendant was represented by Greenberg Traurig LLP and Jones Day LLP.

[38]Because the Court found that the record did not establish the third *Howey* element as to the Programmatic Sales, the Court did not reach whether the first or second *Howey* elements were satisfied. *See* MSJ Decision at 25 n. 17.

[39]*Id.* at 26. Because the Court determined that the record did not establish the first *Howey* element as to the Other Distributions, the Court did not reach whether the second or third *Howey* prongs were satisfied. See id. at 27 n. 18.

[40]*See id.* at 29.

[41]*Id.* at 31.

[42]*Id.* at 13.

EU'S PROPOSED REVISIONS TO THE PAYMENT SERVICES DIRECTIVE, AND HOW THEY COMPARE TO THE UK'S APPROACH

By Azad Ali, Olivia Moul, and David Y. Wang

Azad Ali is of counsel, Olivia Moul is a trainee solicitor, and David Wang is an associate in the London office of Skadden, Arps, Slate, Meagher & Flom LLP.
Contact: azad.ali@skadden.com or olivia.moul@skadden.com or david.y.wang@skadden.com.

On June 28, 2023, the European Commission ("EC") published its proposals for both a revised Payment Services Directive ("PSD3") and a new accompanying Payment Services Regulation ("EU PSR"). This package of reforms addresses certain key issues arising from the operation of the Second Payment Services Directive ("PSD2") and sets out specific enhancements to PSD2.

As a directive, PSD3 will require transposition into member states' national legislation. The EU PSR, in contrast, will be directly applicable, with no implementation required. The intention of the directly applicable regulation is

to mitigate member states' divergent interpretational approaches to certain aspects of PSD2.

Among other things, the proposed updates to PSD2 include:

- A merger of the regimes applicable to e-money institutions ("EMIs") and payment institutions ("PIs"). This simplifies and harmonizes these two very similar regimes, with PIs being authorized to offer e-money services as part of their wider payment services business.
- An extension of fraud protection measures, including: IBAN/name-matching verification for euro-denominated instant payments and refunds for customers who fall victim due to lack of such verification and, subject to some exceptions, to impersonation fraud.
- Clarifications to Strong Customer Authentication ("SCA") requirements, including that SCA be conducted by underlying account providers such as banks only once at the outset, when access is sought by open banking account information service providers.
- Various transparency reforms relating to costs and charges for remittances to non-EU countries and ATM withdrawal charges.
- Reforms to Open Banking: Banks will no longer need to maintain two data access interfaces (a dedicated and a "fallback interface") for customer data, and contingent data access could possibly include the use of the interface banks for their customers. The EC is also presenting proposals in a separate regulation on wider financial data access, expanding beyond account information to other financial products, thereby broadening the scope of Open Banking to wider Open Finance.
- Improvement to access by PIs to bank account services, by requiring banks to justify refusal of such services on specific grounds.

THE UK REGIME

In the UK, PSD2 was implemented by way of the Payment Services Regulations 2017 ("UK PSRs"). The UK has been more advanced that its continental counterparts in respect of certain aspects of the payment services landscape. Notably, it has embraced Open Banking through the work of the Open Banking Implementation Entity ("OBIE") and by encouraging a strong ecosystem of fintech firms in the UK.

The future of Open Banking In the"UK w'll be overseen by the Joint Regulatory Oversight Committee ("JROC"), comprised of representatives from the Financial Conduct Authority ("FCA"), the Payment Systems Regulator, HM Treasury and the Competition and Markets Authority ("CMA"). In January 2023, HM Treasury issued a consultation on the UK PSRs,[1] in which it recognized certain areas for review. Some of these areas are also addressed in the proposed PSD3 and EU PSR, but overall, the UK can be said to be pursuing its own path to reforming and evolving the UK payment services regulatory framework.

COMPARISON OF EU AND THE UK REFORMS OF PSD2

STRONG CUSTOMER AUTHENTICATION

It is well documented that a rise in the use of digital payments and online banking has seen a concomitant increase in fraud. As payment transactions have become increasingly frictionless, the requirements of SCA (a form of regulatory, two-factor authentication) prescribed by PSD2 have sought to ensure greater protection against fraud for payment transactions in both online and contactless offline payments. These rules have had a significant impact in reducing fraud.

The EC proposals now seek to clarify certain features of SCA rules. For example, payment service providers ("PSPs") must have transaction monitoring mechanisms in place that could, in certain cases, trigger the application of SCA, helping to prevent and detect potentially fraudulent payment transactions.

The proposals require:

- Exempting certain types of transactions from SCA, including those initiated by a merchant.
- Clarifying that the specific amount and payee must be linked to the transaction.
- Requiring banks to apply SCA only once at the outset, when an open banking provider first seeks account information.
- Requiring PIs to ensure that SCA can be performed in circumstances where a user does not have access to a device such as a smartphone.

By comparison, the UK consultation recognized the prescriptiveness of SCA. In particular, there are industry concerns regarding market practice in implementing the standard and the impact on access to payment services to those in certain groups (*e.g.*, to those without a mobile phone or reliable network coverage). In response, the UK government is proposing to introduce a degree of flexibility by considering an outcomes-based approach to authenticating payments. Precise details as to what such an approach might entail are under review.

ENHANCED USER PROTECTION

Push payment fraud is increasingly prevalent. PSD2 provides some protection for customers, as it imposes liability on the part of PIs for unauthorized payment transactions. The UK consultation recognized a lacuna: There is no equivalent legislation for victim reimbursement or PI liability in relation to authorized push payments ("APP") fraud, where the payment transaction is authorized by the user but has been entered into through deception by another—typically, where a fraudster impersonates a bank. Voluntary reimbursement is encouraged (for example the Contingent Reimbursement Model sets out standards for PSPs), but there is a lack of a comprehensive and consistent framework to address such types of fraud. Mandatory reimbursement and potential liability of PIs may be consulted on in due course.

The EU proposes liability to attach to the PI for APP fraud, subject to the user promptly notifying the PI and filing a police report, and

not having been grossly negligent in falling victim to the fraud.

OPEN BANKING AND APIS

Accessibility of third parties to customer data in Open Banking is the subject of much discussion, notably around alternative modes of data access such as screen-scraping and around the quality of dedicated APIs mandated under PSD2.

Screen-scraping is a data collection method that gathers information using a payment service user's log-in details, where the third-party provider ("TPP") acts as if it were the user. This is prohibited under PSD2. Instead, PSD2 required banks and other payment account providers to grant TPPs access to payment account data, as well as the ability to initiate payments, via dedicated application programming interfaces ("APIs") developed by banks for this purpose.

The UK has seen more progress in respect of the use of such APIs and has therefore provided a more conducive environment for account information service ("AIS") and payment initiation service ("PIS") providers to develop. This was assisted by the work of the OBIE,[2] which was tasked with implementing certain competition remedies and oversaw the completion of open and common banking standards (including for APIs) being made available with respect to the nine largest current account providers, impacting 6 million users of services powered by Open Banking technology.

Further developments are expected in the UK, specifically in relation to the requirement for the use of dedicated APIs and prohibiting the use of modified customer APIs, which have been used as fallback solutions should the dedicated APIs fail. This prohibition will not apply to small PIs and small EMIs, but otherwise, an alternative fallback solution will be required within six months of product launch unless an exemption is applied for.[3]

Issues remain, however, in the availability and quality of such APIs. JROC sought to address these issues with the publication of its joint paper in June 2023, which set out high-level principles for banks and registered third parties to follow when agreeing on an API.[4] These include requirements that fees and charges for premium APIs should:

- Broadly reflect relevant long-run costs of providing premium APIs to TPPs.
- Incentivize investment and innovation in premium APIs.
- Incentivize the adoption of Open Banking by both consumers and business.
- Treat TPP service providers fairly.
- Be transparent.

The JROC has already published a final report on recommendations for the next phase of Open Banking in the UK.[5] The report, published in April 2023, sets out the UK's timeline for designing a data collection framework for APIs, which will be submitted to the FCA and Payment Systems Regulator for approval in Q2 2023.

The EU is following suit with its intention to impose more detailed specifications for mini-

mum requirements for Open Banking data interfaces. The EU also will require account providers to put in place more substantial and dedicated APIs (replacing the "dedicated" and "fallback" solutions model currently in place), and encourage a "permissions dashboard" to allow users to manage their granted Open Banking access permissions.

WIDENING ACCESS TO PAYMENT SYSTEMS FOR NONBANK PSPS

In the UK, both banks and nonbank PSPs (such as electronic money institutions) have access to payment systems (such as CHAPS, BACS and Faster Payments in the UK), either as direct or indirect participants. Currently, the UK PSRs explicitly prohibit direct participants in these payment systems from discriminating against admitting PIs as indirect participants, such that payment fintech companies seeking access to payments systems should be afforded equal opportunity to do so, regardless of their size and business structure, as long as they meet certain eligibility criteria as set out in the UK PSRs.

In this regard, the EU's proposals go further than the UK, as they contemplate the possibility of direct participation of payment and e-money institutions to all payment systems themselves. Such direct participation is accompanied by additional clarifications on admissions and risk assessment procedures.

NEXT STEPS

In the EU, both the European Council and the European Parliament will review the EC's proposals in order to agree on final texts, which will become legislation once adopted. A prescribed time frame for member states' implementation of PSD3, as well as the transition period for application of the EU PSR, is yet to be announced.

In the UK, the government continues to monitor the need for policy changes, particularly in relation to enhanced fraud prevention, and safeguarding and providing fair protection of customers when terminating payment services. More broadly, the UK payments services regulatory landscape may be the subject of a significant shift, as the government will expand the Payment Systems Regulator's powers under the new Financial Services and Markets Act 2023. It will also review the UK PSRs following consultation throughout 2023.

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]*See* https://www.skadden.com/-/media/files/publications/2023/07/eus-proposed-revisions-to-the-payment-services-directive/hm-treasury-issued-a-consultation-on-the-uk-psrs.pdf.

[2]*See* https://www.skadden.com/-/media/files/publications/2023/07/eus-proposed-revisions-to-the-payment-services-directive/the-work-of-the-obie.pdf.

[3]*See* https://www.skadden.com/-/media/files/publications/2023/07/eus-proposed-revisions-to-the-payment-services-directive/an-alternative-fallback-solution-will-be-required.pdf.

[4]*See* https://www.fca.org.uk/news/news-stories/joint-regulatory-oversight-committee-com

mercial-pricing-principles-open-banking.

[5]*See* https://www.skadden.com/-/media/files/publications/2023/07/eus-proposed-revisions-to-the-payment-services-directive/a-final-report-on-recommendations-for-the-next-phase-of-open-banking-in-the-uk.pdf.

BANKRUPTCY LITIGATION DEMONSTRATES THE EXTENT OF THE CRYPTO CONTAGION

By Elie J. Worenklein, Emily MacKay and Ruth Ramjit

Elie Worenklein is a counsel, and Emily MacKay and Ruth Ramjit are associates, in the New York office of Debevoise & Plimpton LLP. Contact: eworenklein@debevoise.com or efmackay@debevoise.com or rramjit@debevoise.com.

In the wake of the industry's 2022 "crypto winter," which spiraled into a "cryptopocalyse," industry watchers were focused on the contagion effect of the various crypto-related bankruptcy filings. In particular, starting with the May 2022 collapse of Terra LUNA and its TerraUSD (UST) stablecoin, many market participants had to halt operations, limit withdrawals, or take emergency bailout loans to survive. The focus quickly turned to the potential ripple effect that could result from an entity's collapse due to the interconnected nature of the cryptocurrency industry. On January 3, 2023, the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC") issued a joint statement describing the significant volatility and exposure of vulnerabilities in the crypto-asset sector and identified the "Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements."[1] Exemplifying this concern, after FTX, which was at the time one of the largest digital asset exchanges in the world, filed for bankruptcy, parties particularly worried about the impact on other entities in the industry.[2]

In addition, the highly concentrated nature of the digital asset industry created shockwaves in other industries, and was one of the primary causes for the March 2023 banking crisis related to Silicon Valley Bank, Silvergate Bank and Signature Bank, all of which had significant exposure in the digital asset sphere.[3]

As demonstrated by the below-described web of bankruptcy litigation, the interconnected nature of the cryptocurrency market played a significant role in the numerous bankruptcy filings by crypto-related entities. In addition, several of the claims asserted against fellow debtor entities may be the largest sources of recovery in certain of these Chapter 11 cases, which could have a material impact on the distributions to creditors and link together the fates of different debtor entities.

VOYAGER DIGITAL HOLDINGS, INC.

Voyager Digital Holdings, Inc. ("Voyager") was the first crypto entity to file for Chapter 11 when it filed in the Southern District of New York on July 5, 2022. Voyager was a cryptocur-

rency lender and broker that worked with a number of large institutional investors prior to its bankruptcy filing, including hedge fund Three Aarons Capital, Ltd. ("3AC"), which filed for Chapter 15 bankruptcy on July 2, 2022, in connection with its liquidation in the British Virgin Islands. Prior to its bankruptcy filing, 3AC borrowed about $665 million from Voyager. In connection with Voyager's bankruptcy filing, the company noted that the 3AC loan was one of Voyager's largest outstanding loans and that "nonpayment of the loan to 3AC, coupled with severe industry headwinds, would strain the Company's ability to act as a broker for cryptocurrency assets."[4] Ironically, in response to the liquidity crisis caused by 3AC, Voyager secured an unsecured loan from Alameda Ventures Ltd., an affiliate of FTX, which would later also file for bankruptcy.

While Voyager emerged from bankruptcy on May 19, 2023, the litigation claims with 3AC and Alameda/FTX are its largest open disputes, and will accordingly determine what recovery its creditors will receive In particular, Voyager's creditors will receive distributions from any recovery of its $665 million claim against 3AC.[5] In addition, the Voyager plan contemplates a $445 million holdback for the FTX/Alameda litigation, with recoveries estimated between 40% to 64% on their claims, depending on the outcome of the litigation.[6]

CELSIUS NETWORK LLC

Approximately a week after Voyager filed for bankruptcy, Celsius Network LLC and certain of its affiliates ("Celsius") filed Chapter 11 petitions in bankruptcy court in the Southern District of New York on July 13, 2022. Prior to its filing, Celsius was a cryptocurrency lending platform. Celsius attributed its bankruptcy filing on the "domino-effect" of the crypto industry, including the collapse of 3AC and Voyager. At the time of its bankruptcy filing, Celsius disclosed two loans totaling $75 million to 3AC.[7]

One of Celsius' largest claims is against Core Scientific ("Core"), a bitcoin miner that itself filed for Chapter 11 in bankruptcy court in the Southern District of Texas on December 21, 2022. Celsius asserted over $312 million of claims related to the parties' mining rig hosting agreements.[8] The Core debtors objected to Celsius' claim and the parties have publicly disclosed potential mediation. In addition to highlighting the complex procedural posture of the litigation with two separate Chapter 11 debtors in different jurisdictions and multiple parties-in-interest beyond the respective debtors, the Core creditors committee argued that a final resolution of Celsius' asserted $300 million claim was increasingly important as the Core debtors head toward plan negotiations, because its treatment has "potentially massive implications" for distributions to unsecured creditors and whether there will be any residual value left for equity.[9]

BLOCKFI, INC.

BlockFi, Inc. and eight affiliated debtors ("BlockFi") filed Chapter 11 petitions in bankruptcy court in the District of New Jersey on November 28, 2022. Prior to its filing, BlockFi was a cryptocurrency trading and lending platform. While BlockFi had no direct exposure

to the Celsius and Voyager bankruptcy filings, it disclosed that 3AC was one of BlockFi's largest borrower clients, and that its collapse led to material losses for BlockFi.[10] Accordingly, BlockFi required an infusion of capital and liquidity to withstand the losses from 3AC and certain other borrowers and to satisfy the increase in customer withdrawals. However, due to the unfavorable market and investor pessimism, BlockFi noted that such attempts were largely unsuccessful. BlockFi was able to secure a loan from FTX US for up to $400 million notional amount of cryptocurrencies but, "[t]he offer imposed steep costs on BlockFi personnel and shareholders."[11]

In connection with certain loans to Alameda, Alameda's affiliate Emergent Fidelity Technologies Ltd. ("Emergent") guaranteed its obligations and pledged to BlockFi all of its shares of Class A Robinhood common stock. In January of 2023, the Department of Justice seized the Robinhood shares and approximately $20 million in cash proceeds. Emergent filed for bankruptcy on February 3, 2023, and its bankruptcy case is being administered jointly with FTX and Alameda. In April 2023, the FTX, BlockFi and Emergent debtors announced an agreement to stay the pending litigation in their respective cases over the Robinhood shares and share sale proceeds pending the conclusion of criminal proceedings against FTX founder Sam Bankman-Fried.[12]

On May 12, 2023, BlockFi filed an amended plan and disclosure statement,[13] which stated that a "primary driver" of customer recoveries will be litigation recoveries from "the entities that defrauded us," which include FTX and Alameda, 3AC, and Emergent. BlockFi also disclosed that it is contemplating litigation against Core.[14] In its disclosure statement, BlockFi states that successful litigation could yield prospective high-end recoveries of 90%-100% for certain classes of customer and general unsecured claims.[15] In particular, the debtors stated that "[c]ollectively, the success or failure of this litigation . . . will make a difference of in excess of $1 billion to Clients."[16]

FTX TRADING, LTD.

FTX Trading, Ltd. and 101 affiliated debtors ("FTX") filed Chapter 11 bankruptcy petitions in bankruptcy court in the Southern District of New York on November 11-14, 2022. Prior to its bankruptcy filing, FTX was a cryptocurrency exchange and hedge fund that promoted the liquidity and transacting of coins and tokens, and was the first major cryptocurrency exchange to file bankruptcy. As noted earlier, FTX affiliate Alameda Research offered in June 2022 to provide a $250 million revolving credit facility to bail out crypto trading and lending platform BlockFi, and $500 million in financing to bail out crypto lender Voyager. In addition, FTX was the proposed plan sponsor and purchaser of Voyager's assets, but that purchase agreement was terminated after FTX's bankruptcy filing.

On January 30, 2023, FTX sued Voyager in an effort to claw back $445.8 million in loan repayments that FTX made to Voyager before FTX's bankruptcy filing.[17] After Voyager's bankruptcy filing in July 2022, FTX alleges that it, on Alameda's behalf, paid Voyager $248.8 million in September 2022 and $193.9 million

in October 2022, as well as a $3.2 million interest payment in August 2022. [18] As FTX filed for bankruptcy in November 2022, those payments to Voyager are within the 90-day preference period under Bankruptcy Code section 547 and may therefore be clawed back by the debtor FTX to increase the bankruptcy estate available to its creditors.[19]

On April 5, 2023, Judge Wiles approved Voyager's proposed joint stipulation with FTX and their respective official committees of unsecured creditors.[20] The stipulation contained a framework for resolving certain disputes between the Voyager and FTX estates, including FTX debtor Alameda Research's contested $75 million loan claim against Voyager and $445.8 million preferential transfer adversary complaint. In sum, the parties stipulated that FTX's preference claims against Voyager will be adjudicated in FTX's Chapter 11 case.

GENESIS GLOBAL CAPITAL, LLC

Genesis Global Capital, LLC and two affiliates ("Genesis") filed for Chapter 11 in bankruptcy court in the Southern District of New York on January 19, 2023. Prior to its filing, Genesis was a cryptocurrency lender. Genesis disclosed several factors that contributed to its bankruptcy filing, including significant exposure to 3AC and FTX. In addition, Genesis noted the " 'run on the bank' following FTX Entities' collapse was outsized and severely impacted [Genesis'] available liquidity."[21]

On May 3, 2023, FTX moved for relief from the automatic stay in the Genesis bankruptcy in order to commence avoidance actions against Genesis, similar to the action FTX commenced against Voyager.[22] FTX stated that Genesis received avoidable transfers from FTX in the 90-day period prior to the FTX filing, including (i) the repayment of loans to Genesis by Alameda in the aggregate amount of approximately $1.8 billion; (ii) the pledge of collateral by Alameda to Genesis in the aggregate amount of approximately $273 million; and (iii) the withdrawal of assets by Genesis from the FTX.com exchange in the aggregate amount of approximately $1.6 billion. In addition, the FTX debtors stated that they intend to pursue avoidance claims against Genesis nondebtor affiliate, GGC International, for its withdrawal of approximately $213 million from the FTX.com exchange during the preference period. FTX argued that the claims against the Genesis debtors should be adjudicated in a similar manner to FTX's claims in the Voyager cases.

On June 1, 2023, the Genesis debtors filed a motion to establish procedures and a schedule for estimating the FTX claims against the debtors.[23] FTX debtors filed nine proofs of claim against the Genesis debtors, each asserting various claims totaling over $3.876 billion.[24] According to the Genesis debtors, "the face value of the asserted FTX Claims is more than 250% of the value of the Debtors' liquid assets and equal to approximately 90% of all scheduled claims against [the debtors] combined."[25] Accordingly, Genesis asserted that the claims asserted by FTX should be estimated at $0.00 for purposes of voting, allowance and distribution "to avoid undue delay in the timing and amount of creditor distribu-

tions, and to expeditiously pursue confirmation of a chapter 11 plan."[26]

CONCLUSION

As was feared by many industry participants, including the Federal Reserve, FDIC and OCC, the last 12 months have demonstrated the extensive interconnections among certain crypto-asset participants and the contagion nature of the digital asset industry. The pending bankruptcy cases discussed above, in addition to addressing novel legal issues impacting digital assets, reveal how quickly a troubled entity can spread its distress to other entities in the industry, thereby linking their—and their creditors'—fates.

ENDNOTES:

[1]Federal Reserve, FDIC and OCC, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 3, 2023) https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf; *see also* https://www.debevoisefintechblog.com/2023/01/05/federal-banking-agencies-release-joint-statement-on-crypto-asset-risks-to-banks/.

[2]Matt Levine, *FTX Creates Crypto Contagion*, Bloomberg (November 16, 2022) https://www.bloomberg.com/opinion/articles/2022-11-16/ftx-creates-crypto-contagion#xj4y7vzkg; Nina Bambysheva, Javier Paz, Michael del Castillo and Steven Ehrlich, *The Looming $62 Billion Crypto Contagion*, Forbes (November 14, 2022), https://www.forbes.com/sites/ninabambysheva/2022/11/14/the-looming-62-billion-crypto-contagion/?sh=5f64fe7e61c3.

[3]*See e.g.*, Cong. Rsch. Serv. Insight, IN12148, The Role of Cryptocurrency in the Failures of Silvergate, Silicon Valley, and Signature Banks (2023); MacKenzie Sigalos, *What the failures of Signature, SVB and Silvergate mean for the crypto sector*, CNBC (Mar. 12, 2023), https://www.cnbc.com/2023/03/12/signature-svb-silvergate-failures-effects-on-crypto-sector.html.

[4]*In re Voyager Digital Holdings, Inc., et. al.*, Case No. 22-10943 (MEW) (Bankr. S.D.N.Y. March 10, 2023), Docket 15.

[5]*In re Voyager Digital Holdings, Inc., et. al.*, Case No. 22-10943 (MEW) (Bankr. S.D.N.Y. March 10, 2023), Docket 1166.

[6]*Id.*

[7]*In re Celsius Network LLC, et al.*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. Jul. 14, 2022), Docket 23.

[8]*In re Core Scientific Inc., et. al.,* Case No. 22-90341 (DRJ) (Bankr. S. D. Tex. May 5, 2023), Docket 861.

[9]*In re Core Scientific Inc., et. al.,* Case No. 22-90341 (DRJ) (Bankr. S. D. Tex. May 18, 2023), Docket 894.

[10]*In re BlockFi Inc., et al.*, Case No. 22-19361 (MBK) (Bankr. D.N.J. Nov. 28, 2023), Docket 17.

[11]*Id.*

[12]*In re FTX Trading Ltd., et. al.*, Case No. 22-11068 (JTD) (Bankr. D. Del. Apr. 11, 2023), Docket 1261.

[13]*In re BlockFi Inc., et al.*, Case No. 22-19361 (MBK) (Bankr. D.N.J. May 12, 2023), Docket 874 and 875.

[14]*In re BlockFi Inc., et al.*, Case No. 22-19361 (MBK) (Bankr. D.N.J. May 12, 2023), Docket 874.

[15]*Id.*

[16]*Id.*

[17]*In re FTX Trading Ltd.*, Adv. Pro. No. 23-50084 (JTD) (Bankr. D. Del. Jan. 30, 2023), Docket 1 at ¶ 5.

[18]*Id.* at ¶ 18-22.

[19]*See* 11 U.S.C.A. § 547(b).

[20]*In re Voyager Digital Holdings., et al.*, Case No. 22-10943 (MEW) (Bankr. S.D.N.Y. April 6, 2023), Docket 1266.

[21]*In re Genesis Global Holdco, LLC, et al*, Case No. 23-10063 (SHL) (Bankr. S.D.N.Y. Jan. 20, 2023), Docket 17.

[22]*In re Genesis Global Holdco, LLC., et al.*, Case No: 23-10063 (SHL) (Bankr. S.D.N.Y. May 3, 2023), Docket 289.

[23]*In re Genesis Global Holdco, LLC., et al.*, Case No: 23-10063 (SHL) (Bankr. S.D.N.Y. May 3, 2023), Docket 373.

[24]*Id*. at ¶ 13.

[25]*Id*.

[26]*Id.* at ¶ 18.

TRADE SECRETS AND GENERATIVE AI: PROTECTIVE MEASURES IN AN EVOLVING TECHNOLOGICAL LANDSCAPE

By Carl A. Kukkonen III, Randy Kay, Jonathan M. Linas, Emily J. Tait and Steven M. Zadravecz

Carl Kukkonen and Randy Kay are partners in the San Diego office of Jones Day. Jonathan Linas is a partner in the Chicago office of Jones Day, Emily Tait is a partner in Jones Day's Detroit office and Steven Zadravecz is a partner in Jones Day's Irving, California office. Contact: ckukkonen@jonesday.com or rekay@jonesday.com or jlinas@jonesday.com or etait@jonesday.com or szadravecz@jonesday.com.

The Background: In recent months, artificial intelligence ("AI") platforms have taken the world by storm, introducing new, powerful tools for generating original and useful content based on training data and user prompts.

The Situation: These tools pose a potential threat to a company's trade secrets, as an employee may inadvertently disclose sensitive information by using generative AI applications. This has led some companies to ban the use of these applications for work-related tasks.

Looking Ahead: Although prohibiting the use of generative AI is one solution, there are several possible solutions to reasonably protect one's trade secrets while still taking advantage of generative AI's many benefits.

Generative AI applications such as large language models have emerged as groundbreaking tools for analyzing data and generating work product in all industries. As recent news has shown, however, those tools pose a unique threat to a company's trade secrets. These applications capture and store their inputs to train their models. Once captured, the information input into those applications sometimes cannot be deleted by the user, may be used by the application, and may be reviewed by the company behind the AI application. If an employee inputs a company's trade secret into an AI prompt, that trade secret could be at risk of losing its trade secret protection.

To avoid the consequences of any disclosure arising from the use of an AI system, it is important that companies ensure that they take reasonable measures to protect their trade secrets. This Commentary analyzes potential

measures to protect company trade secrets from employees' uses of generative AI applications.

THE REASONABLE MEASURES OF PROTECTION REQUIREMENT FOR TRADE SECRETS

Trade secrets are invaluable assets for businesses, encompassing proprietary information, formulas, processes, techniques, or customer data that provide a competitive advantage. Unlike patents or copyrights, trade secrets rely on confidentiality and are not formally registered. Maintaining the secrecy of trade secrets is essential for preserving a company's distinctiveness and competitive advantage in the market.

Under the Defend Trade Secrets Act ("DTSA"), the owner of a trade secret must take "reasonable measures to keep such information secret."[1] The Uniform Trade Secret Act and related state trade secret statutes have similar requirements.[2] This requirement is critical because failure to take reasonable measures may result in that sensitive information losing its valuable trade secret status.

The DTSA does not define "reasonable measures"; rather, whether those safeguards are reasonable will depend on the circumstances. The good news is that a party only needs to make "reasonable measures," not all conceivable measures. Thus, in some cases, courts have found that a party took reasonable measures to protect its trade secrets despite inadvertently disclosing them to a customer where the party disclosed the trade secrets as a result of a good-faith mistake and the party took immediate action to maintain the secrecy of the information upon learning of the mistake.[3]

GENERATIVE AI AND THE POTENTIAL FOR UNINTENTIONAL DISCLOSURE OF TRADE SECRETS

Generative AI applications have the enormous potential to increase productivity and create innovate solutions for companies across every industry. For example, in the software industry, there are an increasing number of applications that can parse natural and programming language inputs to generate or test source code. And in the life-sciences sector, AI applications can take amino acid sequences and predict protein structures. With continued innovation in the generative AI space, the potential for and use of such tools will only continue to grow.

Generative AI applications have the ability to autonomously create original content by extrapolating information from a vast amount of data collected both from public sources and received inputs. That collected data is often retained on servers controlled by the company that supports the generative AI applications. However, this data collection process implicates various trade secret concerns for the companies that use these applications. Following reports of sensitive information being leaked to third parties after using generative AI platforms, many businesses have implemented complete bans and restrictions on the use of generative AI at work to protect their proprietary information.

There are three primary concerns with an employee's input of company confidential or other sensitive information as a prompt into a generative AI application: (i) depending on the terms of the corresponding end-user license agreement ("EULA"), the company that supports the generative AI application can potentially review, release, or sell that sensitive information; (ii) the application itself can potentially reuse this sensitive information for third parties by training its responses with the sensitive information; and (iii) a third party may access the sensitive information if the company that supports the generative AI application has a security breach. Moreover, in the event of a disclosure, the employee-user cannot retrieve or delete the sensitive information input into the application and stored in the application's servers and cannot otherwise regulate the use or protection of the sensitive information once disclosed.

Currently, more can be done to protect company trade secrets from disclosure by their employees. It has been reported that 70% of employees using generative AI tools do not report such use to their employer. This situation reflects that many companies have not yet implemented stringent policies in the wake of the generative AI boom. By implementing updated policies for protecting one's trade secrets, companies can better prepare themselves for the growing use of generative AI applications.

MITIGATION STRATEGIES

In addition to a company's standard policies for protecting its trade secrets, there are several solutions to further protect against the disclosure of trade secrets through the use of generative AI:

Blanket Ban. As seen from some recent announcements from large multinationals, one solution to prevent the disclosure of trade secrets through generative AI is to prohibit the use of generative AI for work-related tasks altogether. One way to implement this solution is by preventing employees from downloading the software and from accessing web applications, which would stop most employees from using it. Another implementation is simply to instruct employees not to use the software, which is simpler to implement but less effective in preventing employees from using the software. Regular monitoring and audits can help detect and prevent potential violations. However, both cases require constant maintenance and policing for either to be effective. As the use of generative AI proliferates, this may become impractical. Additionally, companies that ban generative AI completely may be at a competitive disadvantage to companies that allow or encourage the use of generative AI because of its potential benefits.

Robust Access Controls. An alternative to a blanket ban on generative AI is to limit the access and use of it. Companies should already have established protocols to limit access to sensitive data. Similarly, companies should consider establishing protocols to limit who can operate and interact with generative AI systems. In addition to limiting who has access, companies should also consider limiting or reviewing what can be used as inputs to the generative AI applications. For example, software could be

used to prevent the use of certain key words or phrases from being used as inputs. As with a blanket ban, regular monitoring and audits can help detect and prevent potential violations as well. These considerations can also be informed by the corresponding EULAs.

Enterprise Licenses. Companies that choose to allow the use of generative AI should consider obtaining an enterprise license that places restrictions on what the AI provider can do with prompts or other inputs to the system. As an example, a EULA for an individual user subscription might specify that the inputs can be used to train the underlying models for use by third parties. In contrast, enterprise licenses may provide that the inputs either cannot be used to train the underlying models or that such trained models can only be used by the company (to the exclusion of third parties).

Third-Party Protection. In addition to the potential for an employee's use of generative AI, contractors and other third parties may use generative AI. Companies must review their existing contracts and consider whether to implement any of the above policies with regard to these third parties as well.

Employee Education and Awareness. Finally, regardless of whether a company bans, limits, or even encourages the use of generative AI, raising awareness among employees about the importance of trade secret protection and the risks associated with generative AI is crucial. Courts have consistently found that companies have taken reasonable measures to protect their trade secrets by keeping updated employee agreements and policies.[4] Thus, companies should update their employee handbooks, agreements, and policies to address the use of generative AI and conduct training programs to educate staff on handling sensitive information, emphasizing the legal and ethical obligations surrounding trade secrets.

CONCLUSION

The advent of generative AI brings immense opportunities but also poses some obstacles for protecting company confidential information and trade secrets. Whether companies choose to ban, limit, or allow the use of generative AI, they should implement robust security measures, establish clear policies, and foster a culture of awareness to mitigate the risks. By proactively addressing these challenges, businesses can safeguard their valuable intellectual property assets and maintain their competitive edge in the ever-evolving AI landscape.

FIVE KEY TAKEAWAYS

1. Although a ban on generative AI may be the strongest method of preventing disclosure of trade secrets, this solution may be costly to enforce and may result in a competitive disadvantage.

2. Robust limitations on access and inputs to generative AI applications protect sensitive information while taking advantage of generative AI's potential benefits to productivity and innovation.

3. Companies should consider adopting enterprise versions of generative AI applications with EULAs that provide that any data collected is either protected or deleted.

4. Companies must also ensure that all contractors and third parties comply with their generative AI policies.

5. Employee education and awareness are key to protecting one's sensitive information from being inadvertently or unintentionally disclosed using generative AI.

The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect the views or opinions of the law firm with which they are associated.

ENDNOTES:

[1]18 U.S.C.A. § 1839 (3)(A).

[2]*See, e.g.,* Uniform Trade Secrets Act, § 1(4)(ii) (requiring the trade secret to be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy"); Cal. Civ. Code § 3426.1(d)(2) (same); Tex. Civ. Prac. & Rem. Code § 134A.002(6)(B) (requiring "the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret").

[3]*See Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc.*, 147 F. Supp. 2d 1057, 1066-67 (D. Kan. 2001); *see also John Bean Technologies Corporation v. B GSE Group, LLC*, 480 F. Supp. 3d 1274, 1296-99 (D. Utah 2020).

[4]*See, e.g., Philips North America LLC v. Hayes*, 2020 WL 5407796, *9 (D. Md. 2020) (plaintiff plausibly alleged reasonable measures to protect its trade secrets based on reference to "Employee Ethics and Intellectual Property Agreement"); *ExpertConnect, L.L.C. v. Fowler*, 2019 WL 3004161, *4 (S.D. N.Y. 2019) (plaintiff plausibly alleged reasonable measures to protect its trade secrets based in part on reference to employee handbook); *Enterprise Leasing Co. of Phoenix v. Ehmke*, 197 Ariz. 144, 151, 3 P.3d 1064, 1071, 15 I.E.R. Cas. (BNA) 1496, 55 U.S.P.Q.2d 1303, 139 Lab. Cas. (CCH) P 58794 (Ct. App. Div. 1 1999) (finding that a company took reasonable measures to protect its trade secrets by limiting disclosures, including a confidentiality provision in its employment agreements with high-level managers, and including a confidentiality provision in the employee policy handbook).

PARADISE LOST? HOW CRYPTO FAILED TO DELIVER ON ITS PROMISES AND WHAT TO DO ABOUT IT

By Fabio Panetta

Fabio Panetta is a member of the executive board of the European Central Bank. The following is edited from a speech that he gave at the 22nd BIS Annual Conference in Basel, on June 23, 2023.

Some 15 years ago, software developers using the pseudonym Satoshi Nakamoto created the source code of what they thought could be decentralized digital cash.[1] Since then, crypto has relied on constantly creating new narratives to attract new investors, revealing incompatible views of what crypto-assets are or ought to be.

The vision of digital cash—of a decentralized payment infrastructure based on cryptography—went awry when blockchain networks became congested in 2017, resulting in soaring transaction fees.[2]

Subsequently, the narrative of digital gold gained momentum, sparking a "crypto rush" that led to one in five adults in the United States

and one in 10 in Europe speculating on crypto, with a peak market capitalization of €2.5 trillion.[3]

However, this illusion of crypto-assets serving as easy money and a robust store of value dissipated with the onset of the crypto winter in November 2021. The fall in the price of cryptos led to a decrease of around €2 trillion worth of crypto assets within less than a year. This caught millions of investors unprepared.[4] An estimated three-quarters of bitcoin users suffered losses on their initial investments at this time.[5]

Understandably, many are now questioning the future of crypto-assets. But the bursting of the bubble does not necessarily spell the end of crypto-assets.[6] People like to gamble and investing in crypto offers them a way to do so.[7]

Crypto valuations are highly volatile, reflecting the absence of any intrinsic value. This makes them particularly sensitive to changes in risk appetite and market narratives. The recent developments that have affected leading crypto-asset exchanges have highlighted the contradictions of a system which, though created to counteract the centralization of the financial system, has become highly centralized itself. I contend that due to their limitations, cryptos have not developed into a form of finance that is innovative and robust, but have instead morphed into one that is deleterious. The crypto ecosystem is riddled with market failures and negative externalities, and it is bound to experience further market disruptions unless proper regulatory safeguards are put in place.

Policymakers should be wary of supporting an industry that has so far produced no societal benefits and is increasingly trying to integrate into the traditional financial system, both to acquire legitimacy as part of that system and to piggyback on it. Instead, regulators should subject cryptos to rigorous regulatory standards, address their social cost, and treat unsound crypto models for what they truly are: a form of gambling.

This may prompt the ecosystem to make more effort to provide genuine value in the field of digital finance.

SHIFTING NARRATIVES: FROM DECENTRALIZED PAYMENTS TO CENTRALIZED GAMBLING

The core promise of cryptos is to replace trust with technology, contending that the concept "code is law" will allow a self-policing system to emerge, free of human judgement and error. This would in turn make it possible for money and finance to operate without trusted intermediaries.

However, this narrative often obfuscates reality. Unbacked cryptos have made no inroads into the conventional role of money. And they have progressively moved away from their original goal of decentralization to increasingly rely on centralized solutions and market structures. They have become speculative assets,[8] as well as a means of circumventing capital controls, sanctions or financial regulation.

BLOCKCHAIN LIMITATIONS

A key reason why cryptos have failed to make good on their claim to perform the role of money is technical. Indeed, the use of blockchain—particularly in the form of public, permissionless blockchain—for transacting crypto-assets has exhibited significant limitations.[9]

Transacting cryptos on blockchains can be inefficient, slow and expensive; they face the blockchain trilemma, whereby aiming for optimal levels of security, scalability and decentralization at the same time is not achievable.[10]

Crypto-assets relying on a proof-of-work validation mechanism, which is especially relevant for bitcoin as the largest crypto-asset by market capitalization,[11] are ecologically detrimental. Public authorities will therefore need to evaluate whether the outsized carbon footprint of certain crypto-assets undermines their green transition commitments.[12] Moreover, proof-of-work validation mechanisms are inadequate for large-scale use.[13] Bitcoin, for example, can only accommodate up to seven transactions per second and fees can be exorbitant.

While alternative solutions to overcome the blockchain trilemma and proof-of-work consensus shortcomings have emerged for faster and more affordable transactions, including those outside the blockchain, they have drawbacks of their own. "Off-chain" transactions conducted via third-party platforms compromise the core principles of crypto-assets, including security, validity and immutability.[14] Another important aspect is the operational risk inherent in public blockchains due to the absence of an accountable central governance body that manages operations, incidents or code errors.[15]

Moreover, the handling of crypto-assets can be challenging. In a decentralized blockchain, users must protect their personal keys using self-custody wallets, which can discourage widespread adoption due to the tasks and risks involved, for example the theft or loss of a key. Given the immutability of blockchains, they do not permit transaction reversal.[16]

INSTABILITY

Another key limitation of unbacked cryptos is their instability.

Unbacked cryptos lack intrinsic value and have no backing reserves or price stabilization mechanisms.[17] This makes them inherently highly volatile and unsuitable as a means of payment. Bitcoin, for instance, exhibits volatility levels up to four times higher than stocks, or gold. Such high volatility also means that households cannot rely on crypto-assets as a store of value to smooth their consumption over time. Similarly, firms cannot rely on crypto-assets as a unit of account for the calculation of prices or for their balance sheet.

Moreover, unbacked cryptos do not improve our capacity to hedge against inflation. Indeed, their price developments exhibit an increasing correlation with stock markets. And empirical analysis finds that momentum in the crypto-asset market and global financial market volatility do have an impact on bitcoin trading against fiat currencies.[18]

CRYPTOS AS A MEANS OF GAMBLING AND CIRCUMVENTION

But the very instability of unbacked cryptos does make them appealing as a means of gambling. And their use as such has been facilitated by the establishment of a centralized market structure that supports the broader use of crypto-assets.[19]

Crypto exchanges have become gateways into the crypto ecosystem, often providing user access to crypto markets in conjunction with other services like wallets, custody, staking[20] or lending. Off-chain grids or third-party platforms have offered users easy and cost-effective ways to engage in trading and speculation, while stablecoins are being used to bridge the gap between fiat and crypto by promising a stable value relative to fiat currency.[21]

Besides gambling, crypto assets are also being used for bypassing capital controls, sanctions and traditional financial regulation. A prime example is bitcoin, which is used to circumvent taxes and regulations, in particular to evade restrictions on international capital flows and foreign exchange transactions, including on remittances.[22] These practices may have destabilizing macroeconomic implications in some jurisdictions, notably in developing and emerging markets.

RISKS FROM GROWING CENTRALIZATION OF THE CRYPTO ECOSYSTEM

The crypto ecosystem's move away from its original goals towards more centralized forms of organization, typically without regulatory oversight, is giving rise to substantial costs and an array of contradictions. There are two major facets to this phenomenon.

THE RE-EMERGENCE OF CLASSIC FINANCIAL SECTOR SHORTCOMINGS AND VULNERABILITIES

First, dependence on third-party intermediaries, many of which are still unregulated, has resulted in market failures and negative externalities, which crypto was initially designed to sidestep.

The crypto ecosystem, for instance, has cultivated its own concentration risks, with stablecoins assuming a key role in trading and liquidity provision within decentralized finance markets.[23] The difficulties faced by prominent stablecoins in the past year likely contributed significantly to the noticeable downturn in these markets.[24]

Indeed, stablecoins often pose greater risks than initially thought. They introduce into the crypto space the kind of maturity mismatches commonly seen in money market mutual funds. As we have seen in the past year, redemption at par at all times is not guaranteed, risks of runs and contagion are omnipresent, and liquidation of reserve assets can lead to procyclical effects through collateral chains across the crypto ecosystem.

Another episode of instability driven by high concentration risk was the fall of the crypto exchange FTX. Initially the crisis seemed to

primarily affect liquidity, but it quickly evolved into a solvency crisis. This situation arose due to FTX's inadequate risk management, unclear business boundaries and mishandling of customer funds. The repercussions of this event rippled through the crypto ecosystem, causing cascading liquidations[25] that underscored the interconnectedness and opacity of crypto markets. Ultimately, it showcased how swiftly confidence in the industry could deteriorate.

Similarities to the FTX case can be seen in the recent civil charges brought by the US Securities and Exchange Commission against the biggest remaining crypto exchange: Binance. These civil charges allege that Binance's CEO and Binance entities were involved in an extensive web of deception, conflicts of interest, lack of disclosure and calculated evasion of the law.[26] Should these allegations be proven, this would be yet another example of the fundamental shortcomings of the crypto ecosystem.

The recent crypto failures also show that risk, in itself, is technology-neutral. In financial services, it does not matter if a business ledger is kept on paper as it was for hundreds of years, in a centralized system as we have now or on a blockchain as in the crypto asset ecosystem. In the end, whether a firm remains in business or fails depends on how it manages credit risk, market risk, liquidity risk and leverage. Crypto enthusiasts would do well to remember that new technology does not make financial risk disappear. The financial risk either remains or transforms into a different type. It is like pressing a balloon on one side: it will change in shape until it pops on the other side. And if the balloon is full of hot air, it may rise for a while but will burst in the end.

LINKS WITH THE TRADITIONAL FINANCIAL SECTOR

The second contradiction arises from the crypto industry's attempt to strengthen ties with actors in the financial system, including banks, big tech companies and the public sector.

Major payment networks[27] and intermediaries[28] have enhanced their support services for crypto-assets. Numerous prominent tech companies, including Meta (formerly Facebook) and Twitter, have explored ways to incorporate crypto into their platforms.[29] By leveraging their large customer base and offering a mix of payments and other financial services, tech firms, especially big techs, could solidify the ties between crypto-assets and the financial system.

The recent failures of Silvergate Bank and Signature Bank have highlighted the risks for banks associated with raising deposits from the crypto sector. The stability of these deposits is questionable given cryptos' volatility. The discontinuation of the Silvergate Exchange Network and SigNet, which functioned as a quasi-payment system for the crypto investments of Silvergate Bank and Signature Bank clients, also shows how crypto-assets service providers depend on the traditional financial sector for settlement in fiat money.

The crypto industry not only seeks to strengthen its ties with the traditional financial industry. It also seeks to gain access to the public safety net that strongly regulated financial

entities benefit from.[30] Indeed, Circle, the issuer of the USD Coin ("USDC") tried to gain access to the Federal Reserve's overnight reverse repurchasing facility in order to back its stablecoin.[31]

The crypto industry is seeking to grow by parasitizing the financial system: it touts itself as an alternative to the financial sector, yet it seeks shelter within that very sector to address its inherent risks, all in the absence of adequate regulatory safeguards.

THE PUBLIC RESPONSE: BACKING, REGULATING OR INNOVATING?

The public sector response can be encapsulated in three main suggestions.

NOT GIVING IN TO THE TEMPTATION TO OFFER PUBLIC BACKING TO CRYPTOS

First, the temptation to offer public backing to cryptos must be resisted. The idea of permitting stablecoin issuers as non-bank financial institutions to hold their reserves at central banks might seem appealing, but could lead to serious adverse consequences.

By granting stablecoins access to the central bank's balance sheet, we would effectively outsource the provision of central bank money. If the stablecoin issuer were able to invest its reserve assets[32] in the form of risk-free deposits at the central bank, this would eliminate the investment risks that ultimately fall on the shoulders of stablecoin holders. And the stablecoin issuer could offer the stablecoin holders a means of payment that would be a close substitute for central bank money.[33]

This would compromise monetary sovereignty, financial stability and the smooth operation of the payment system. For example, a stablecoin could displace sovereign money by using the large customer network of a big tech, with far-reaching implications.[34] Therefore, central banks should exercise prudence and retain control over their balance sheet and the money supply.

REGULATING CRYPTOS ADEQUATELY AND COMPREHENSIVELY

Second, regulators should refrain from implying that regulation can transform crypto-assets into safe assets. Efforts to legitimize unsound crypto models in a bid to attract crypto activities should be avoided.[35]

Moreover, the principle of "same activity, same risk, same regulation" should be endorsed. Cryptos cannot become as safe as other assets and investors should be aware of the risks. Anti-money laundering/countering the financing of terrorism rules should be enforced, and crypto activities of traditional firms should be carefully monitored.

While some jurisdictions attempt to apply existing regulatory frameworks to crypto-assets, the EU's Markets in Crypto-Assets Regulation offers a customized regulatory structure that applies to all 27 EU Member States and draws on existing regulation where appropriate (e-money being one example). The EU has also updated existing regulation, for

instance by extending the travel rule to crypto transactions.[36]

Despite the EU taking the lead in establishing a comprehensive framework regulating crypto activities, further steps are necessary. All activities related to the crypto industry should be regulated, including decentralized finance activities like crypto-asset lending or non-custodial wallet services.[37] Moreover, the regulatory framework for unbacked crypto-assets may be deemed lighter than for stablecoins as it relies mainly on disclosure requirements for issuing white papers,[38] and on the supervision of the service providers which will offer them for trading. The risks posed by unbacked crypto-assets, which are largely used for speculative purposes, should be fully recognized. Enhancing transparency and awareness of the risks associated with crypto-assets and their social cost are critical aspects of this approach. Public authorities will also need to address those social costs: for instance, cryptos' ecological footprint cannot be ignored in view of environmental challenges.

Additionally, the experience of FTX, which expanded massively with little oversight, underscores the importance of global crypto regulation and regulatory cooperation. The Financial Stability Board's recommendations[39] for the regulation and oversight of crypto-asset activities and markets need to be finalized and implemented urgently, also in non-FSB jurisdictions. The Basel Committee on Banking Supervision's standard on the prudential treatment of banks' crypto-asset exposures is a positive step in this direction. It stipulates conservative capital requirements for unbacked crypto-assets with a risk weight of 1,250%, as well as an exposure limit constraining the total amount of unbacked crypto a bank can hold to generally below 1% of Tier 1 capital. It will be key for the European Union and other Basel jurisdictions to transpose the Basel standard into their legislation by the 1 January 2025 deadline.[40]

However, regulation alone will not be sufficient.

INNOVATING: DIGITAL SETTLEMENT ASSETS AND CENTRAL BANK DIGITAL CURRENCIES

Third, the public sector needs to contribute to the development of reliable digital settlement assets.

Central banks are innovating to provide a stability anchor that maintains trust in all forms of money in the digital age. Central bank money for retail use is currently only available in physical form—cash. But the digitization of payments is diminishing the role of cash and its capacity to provide an effective monetary anchor. A central bank digital currency would offer a digital, risk-free standard and facilitate convertibility among different forms of private digital money. It would uphold the singleness of money and protect monetary sovereignty. We are advancing with our digital euro project and aim to complete our investigation phase later this year.

Furthermore, the tokenization of digital finance may require central banks to modify their technological infrastructure supporting the issuance of central bank money for wholesale transactions. This could involve establishing a

bridge between market distributed ledger technology ("DLT") platforms and central bank infrastructures, or a new DLT-based wholesale settlement service with DLT-based central bank money.[41] We will involve the market in the exploratory work that we have recently announced.[42]

CONCLUSION

To conclude, crypto-assets have been promoted as decentralized alternatives promising more resilient financial services. However, the reality does not live up to that promise. The blockchain technology underpinning crypto-assets can be extremely slow, energy-intensive and insufficiently scalable. The practicality of crypto-assets for everyday transactions is low due to their complex handling and significant price volatility.

To address these drawbacks, the crypto ecosystem has changed its narrative, favoring more centralized forms of organization that emphasize crypto speculation and quick profit. But recent events have exposed the fragility of the crypto ecosystem, demonstrating how quickly confidence in crypto-assets can evaporate. In many respects, this ecosystem has recreated the very shortcomings and vulnerabilities that blockchain technology initially intended to address.

Further complicating matters, the crypto market seeks integration into the financial sector for increased relevance and public sector support. This would not provide the basis of a sustainable future for crypto. If anything, it would only heighten contradictions and vulnerabilities, resulting in greater instability and centralization.

The public sector should adopt a determined position by establishing a comprehensive regulatory framework that addresses the social and environmental risks associated with crypto, including the use of unbacked crypto-assets for speculative purposes. It should also resist calls to provide state backing for cryptos, which would essentially socialize crypto risks. The public sector should instead focus its efforts on contributing to the development of reliable digital settlement assets, including through their work on central bank digital currencies.

Decisive action of this kind should motivate the crypto ecosystem, including its foundational technology, the blockchain, to realign its objectives towards delivering real economic value within the digital finance landscape.

ENDNOTES:

[1]Panetta's full speech can be found at https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230623_1~80751450e6.en.html. *See* Nakamoto, S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org.

[2]To maintain a system of decentralized consensus on a blockchain, self-interested validators need to be rewarded for recording transactions. In order to achieve sufficiently high rewards, the number of transactions per block needs to be limited. As transactions near this limit, congestion increases the cost of transactions exponentially. *See* Boissay et al., "Blockchain scalability and the fragmentation of crypto," BIS Bulletin, No 56, Bank for International Settlements, June 7, 2022.

[3]It should be noted that holdings of crypto-assets are often concentrated in the hands of a

few holders who could influence supply and prices. Moreover, some investments are the proceeds of illicit activities, which may be price elastic.

[4]The market capitalization of crypto-assets decreased from its peak of around €2.68 trillion on November 10, 2021 to €801 billion on July 2, 2022. By June 14, 2023, it stood at €978 billion. Source: CoinMarketCap.

[5]*See* Auer et al., "Crypto trading and Bitcoin prices: evidence from a new database of retail adoption," BIS Working Papers, No 1049, Bank for International Settlements, November 2022.

[6]*See* Panetta, F., "Caveat emptor does not apply to crypto," The ECB Blog, January 5, 2023.

[7]*See* Panetta, F., "Crypto dominos: the bursting crypto bubbles and the destiny of digital finance," speech at the Insight Summit, London Business School, December 7, 2022.

[8]Incidences of fraud, human error and manipulation have eroded the trust of crypto enthusiasts, leading to calls for scrutiny, oversight and public intervention. Research and analysis show that fully decentralized set-ups are often concentrated on few holders or require other types of human intervention. This makes them prone to manipulation and risks. *See* for example, Sayeed and Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," Applied Sciences, Vol. 9, No 9, April 2019.

[9]Blockchain technology may however be well-suited to other areas, for instance, supply chain management.

[10]*See* S. Shukla,, The 'Blockchain Trilemma' That's Holding Back Crypto, The Washington Post, September 11, 2022.

[11]As of June 14 bitcoin had a market capitalization of €465.92 billion. Source: CoinGecko.

[12]*See* Gschossmann, I. van der Kraaij, A., Benoit, P-L. and Rocher, E., "Mining the environment—is climate risk priced into crypto-assets?," ECB Macroprudential Bulletin, July 11, 2022.

[13]Moreover, Makarov and Schoar show that bitcoin mining is highly concentrated: the top 10% of miners control 90% of mining capacity and just 0.1% (about 50 miners) control close to 50% of mining capacity. Alternatively, blockchains based on proof of stake are faster, but also tend towards centralization, as larger coin holders can reap more rewards, concentrating power and the risk of 51% attacks. *See* Makarov, I. and Schoar, A., "Blockchain Analysis of the Bitcoin Market," NBER Working Papers, No 29396, National Bureau of Economic Research, April 18, 2022.

[14]*See* Soares, X., "On-Chain vs. Off-Chain Transactions: What's the Difference?," CoinDesk, May 11, 2023.

[15]*See* Walch, A. (2018), "Chapter 11—Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?," in Chuen, D.L.K. and Deng, R. (eds.), Handbook of Blockchain, Digital Finance, and Inclusion, Vol. 2, Academic Press, pp. 243-269.

[16]Moreover, the fact that data stored on the blockchain is immutable and transparent may put the technology in conflict with digital privacy rights.

[17]In the absence of flexible supply mechanisms, unbacked cryptos are incapable of effectively responding to temporary fluctuations in demand and thus fail to stabilize their value. Similarly, bitcoin's limited supply—at 21 million coins—means that it does not offer protection against the risk of structural deflation.

[18]Di Casola, P., Habib, M. and Tercero-Lucas, D. (2023), "Global and local drivers of Bitcoin trading vis-á-vis fiat currencies," ECB Working Paper Series, forthcoming.

[19]The industry's trend towards centralization is clear. Since 2015 approximately 75% of the actual bitcoin volume has been associated with exchanges or exchange-like entities, including online wallets, over-the-counter (OTC)

desks and large institutional traders. *See* Makarov and Schoar (2022), op. cit.

[20]Staking is the foundation of the proof-of-stake consensus mechanism, which entails individuals locking up their assets (native coins) on a blockchain to secure the protocol. The stake acts as a form of collateral to ensure that validators, who are responsible for verifying and appending the blockchain, act in a manner that is in line with the protocol's rules. *See* Oderbolz, N., Marosvölgyi, B. and Hafner, M., "The Economics of Crypto Staking," Swiss Economics Blog, March 1, 2023.

[21]They back their value with securities, commodities, as well as fiat money. Interestingly and inevitably, major stablecoin issuers—such as Tether or Circle—adopt centralized organizational structures, directly contradicting the initial ideas as laid down in Satoshi Nakamoto's white paper. The notion that stablecoin issuers might invest in crypto-assets could further concentrate holdings and contradict the low-risk requirements for stablecoin reserves.

[22]Graf von Luckner, C., Reinhart, C.M. and Rogoff, K., "Decrypting new age international capital flows," Journal of Monetary Economics, June 1, 2023.

[23]Although it represents only a small part of the crypto-asset market, the stablecoin Tether accounts for close to half of all trading on crypto-asset trading platforms. *See* the section entitled "Stablecoins' role within the crypto-asset ecosystem" in Adachi, M. et al. (2022), "Stablecoins' role in crypto and beyond: functions, risks and policy," Macroprudential Bulletin, Issue 18, ECB.

[24]*See* the May 2023 report by the ESRB Task Force on Crypto-Assets and Decentralised Finance entitled "Crypto-assets and decentralised finance."

[25]A decentralized finance ecosystem is built around crypto lending that is collateralized by other crypto-assets, using smart contracts to implement margin calls. The failure of FTX had a large impact on the price of crypto-assets serving as collateral for crypto lending. This triggered cascading liquidations by crypto lenders because of the decrease in the value of the collateral.

[26]*See* US Securities and Exchange Commission, SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao, June 5, 2023.

[27]In particular, Mastercard, PayPal and Visa continue building capabilities and strategic partnerships to support crypto-assets (as well as stablecoins).

[28]*See*, for example, JP Morgan's Onyx Coin Systems Product Team, Fidelity's Fidelity Crypto? account and Citi's collaboration with METACO to develop and pilot digital asset custody capabilities.

[29]Meta expressed interest in the metaverse and the potential integration of crypto-assets and blockchain technology within its virtual reality platform. The company has been exploring the concept of a blockchain-based digital currency called "Facebook Diem" (previously known as Libra). Twitter has integrated bitcoin tipping features. It allows users to send and receive bitcoin tips to content creators and other users on the platform.

[30]*See* PYMTS (2023), Circle Says Lack of Direct EMI Access to EU Central Bank Accounts Stifles Payments Innovation.

[31]Circle's USD 31 billion USDC stablecoin maintains around USD 25 billion of its reserves in short-term US Treasury bills in the exclusive Circle Reserve Fund, managed by BlackRock. The fund is registered as a "2a-7" government money market fund. Circle's objective for the fund was to secure access to the Federal Reserve's reverse repurchasing facility through BlackRock, allowing the company to move USDC's remaining cash reserves from partner banks to the fund under a Federal Reserve account.

[32]Reserve assets are the assets against which the stablecoins are valued and redeemed.

[33]In contrast, the substitutability between

central bank money and bank deposits is limited by the fact that, on bank balance sheets, deposits are matched against risky assets (bank loans).

[34]*See* Panetta, F., "From the payments revolution to the reinvention of money," speech at the Deutsche Bundesbank conference on the "Future of Payments in Europe," November 27, 2020.

[35]*See* Chipolina, S. and Asgari, N., "Binance slams US crypto crackdown and makes bid for UK oversight," Financial Times, May 10, 2023.

[36]The "travel rule," already used in traditional finance, will in the future cover transfers of crypto-assets. Information on the source of the asset and its beneficiary will have to "travel" with the transaction and be stored on both sides of the transfer. The law also covers transactions above €1,000 from "self-hosted wallets" (a crypto-asset wallet address of a private user) when they interact with hosted wallets managed by crypto-asset service providers. *See* Regulation (EU) 2023/1113 of the European Parliament and of the Council of May 31, 2023, on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance), Official Journal L 150, June 9, 2023, p. 1-39.

[37]Crypto lending is a centralized or decentralized finance service that allows investors to lend out their crypto holdings to borrowers. Decentralized crypto lending platforms use smart contracts to automate loan payouts and yields, and users can deposit collateral to receive a loan if they meet the appropriate requirements automatically (*see* Duggan, W., "Crypto Lending: Earn Money From Your Crypto Holdings," Forbes, January 30, 2023). A non-custodial wallet, or self-custody wallet, entails the crypto owner being fully responsible for managing their own cryptos. The users have full control of their crypto holdings, manage their own private key and handle transactions themselves (*see* "Custodial vs Non-Custodial Wallets," crypto.com, February 17, 2023).

[38]This is a sort of prospectus for crypto-assets that informs potential holders about the characteristics of the issued crypto-asset before they offer a token to the public or list it on a trading platform.

[39]*See* Financial Stability Board (2023), "Crypto-assets and Global "Stablecoins."

[40]*See* European Central Bank, "Crypto-assets: a new standard for banks," Supervision Newsletter, February 15, 2023.

[41]Panetta, F., "Demystifying wholesale central bank digital currency," speech at the Deutsche Bundesbank's Symposium on "Payments and Securities Settlement in Europe-today and tomorrow," Frankfurt am Main, September 26, 2022.

[42]European Central Bank, "Eurosystem to explore new technologies for wholesale central bank money settlement," Frankfurt am Main, April 28, 2023.

FINTECH LAW REPORT: JUNE/JULY 2023 REGULATION AND LITIGATION UPDATE

By Duncan Douglass and Nate Tyre

Duncan Douglass is a partner and the head of the payment systems practice at the law firm Alston & Bird, LLP. Nate Tyre is an associate in the same firm. www.alston.com.

REGULATORY DEVELOPMENTS

CFPB Releases Report on Deposit Insurance Coverage on Non-Bank Payment Platforms and Related Consumer Advisory

On June 1, 2023, the Consumer Financial Protection Bureau (the "CFPB") Office of Competition and Innovation and Office of

Markets published an issue spotlight report on the risks consumers face in holding their funds in nonbank, peer-to-peer payment platforms (*e.g.*, PayPal, Venmo, CashApp, and others) (the "Payment Apps"), which "claim to provide federal deposit insurance" (the "Payment App Report").[1] Specifically, the Payment App Report concludes that consumer funds stored in a Payment App "may be at significantly higher risk of loss for a consumer than if it is deposited in an insured bank or credit union account."[2]

According to the Payment App Report, the Payment Apps offer consumers financial services and products similar to traditional banks—payment transfer and stored value services—without offering similar protections, notably individual deposit insurance. The Payment App Report estimates that consumers have "billions of dollars stored" on these Payment Apps.[3]

The CFPB asserts that the Payment Apps' user agreements are "often confusing, murky, or even silent on" where consumer funds are held and whether they are protected by deposit insurance. The Payment App Report highlights products offered by PayPal, Venmo, CashApp, Apple Pay, and Google Pay to compare the representations made regarding deposit insurance and where consumer funds are held. Regarding deposit insurance eligibility, PayPal, Venmo, CashApp, and Apple Pay represent that consumers must participate in additional service offerings to potentially be eligible for deposit insurance (*e.g.*, opening a debit or prepaid card account, enrolling in direct deposit, using the account to buy or receive crypto assets, or registering the account with a sponsor bank), with deposit insurance eligibility ultimately subject to Federal Deposit Insurance Corporation (the "FDIC") rules. Google Pay makes no deposit insurance representations.[4]

Further, the CFPB notes that the Payment Apps often are regulated as money services businesses under state and federal laws, however the CFPB suggests these laws, which were designed for traditional money transfer providers like Western Union and MoneyGram that do not store funds for any length of time, do not provide sufficient consumer protection for those who use and store funds with Payment Apps.[5]

On June 1, 2023, the CFPB also published a consumer advisory based on the findings published in the Payment App Report (the "Payment App Advisory").[6] The Payment App Advisory describes that a consumer is at greater risk when their funds remain in the Payment Apps because the money held in the Payment App might not be insured, therefore in the event a Payment App suffers a business failure or bankruptcy, the consumer may lose their funds or not have access to their funds for a long time. Additionally, the Payment App Advisory makes note that some Payment Apps may offer additional coverage through pass-through deposit insurance only for consumers who engage in additional services, such as direct deposit. The Payment App Advisory clarifies that pass-through deposit insurance protects consumers against the failure of a bank or credit union that has a business arrangement with a Payment App, but does not protect the consumer against the failure of the Payment App itself.

You can access the Payment App Report

here: https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/full-report/.

You can access the Payment App Advisory here: https://www.consumerfinance.gov/about-us/newsroom/consumer-advisory-your-money-is-at-greater-risk-when-you-hold-it-in-a-payment-app-instead-of-moving-it-to-an-account-with-deposit-insurance/.

Federal Banking Agencies Issue Final Guidance on Third-Party Relationship Risk Management

On June 6, 2023, the Board, the FDIC, and the Office of the Comptroller of the Currency (the "OCC" and together with the Board and the FDIC, the "Federal Banking Agencies") issued final Interagency Guidance on Third-Party Relationships: Risk Management (the "Final Third-Party Guidance").[7] The Final Third-Party Guidance follows nearly two years after the Federal Banking Agencies initially proposed interagency guidance on managing risks associated with third-party relationships (the "Proposed Third-Party Guidance") and incorporates changes based on comments received on the Proposed Third-Party Guidance.[8] The Final Third-Party Guidance became effective upon its publication and supersedes each of the Federal Banking Agencies' existing third-party risk management guidance, including the Board's 2013 guidance, the FDIC's 2008 guidance, the OCC's 2013 guidance (the "2013 OCC Guidance"),[9] and the OCC's 2020 frequently asked questions (the "OCC FAQs").

The Final Third-Party Guidance is intended to "promote consistency in supervisory approaches" and "offers the agencies' views on sound risk management principles for banking organizations when developing and implementing risk management practices for all stages in the life cycle of third-party relationships," while recognizing that "sound third-party risk management takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship."[10]

The Proposed Third-Party Guidance is largely based on the 2013 OCC Guidance and OCC FAQs, updated to: (i) replace certain prescriptive guidance with general best practice statements; (ii) provide that risk-commensurate analysis should be performed by "those with the requisite knowledge and skills" (including, when internal resources are limited, by the engagement of industry experts) with appropriate management involvement in the negotiation and execution of vendor contracts, including board involvement in the approval of contracts involving critical activities; and (iii) the expansion of due diligence standards.[11]

The Federal Banking Agencies emphasize that the Final Third-Party Guidance is not a standard, law or regulation, but rather a set of "key principles banking organizations can leverage when developing and implementing risk management processes tailored to the risk profile and complexity of their third-party relationships."[12] Responding to comments received, the Federal Banking Agencies made certain changes and clarifications to the Proposed Third-Party Guidance, a number of which were accomplished by incorporating

concepts from the OCC FAQs. Key changes included in the Final Third-Party Guidance include:

- Incorporating concepts from OCC FAQs 1 and 2, clarifying that the terms "business arrangement" and "third-party relationship" are broad by design, that risk management practices should vary according to the nature of the relationship, and that "business arrangements" may include some relationships that have features of a customer relationship.
- Revising the term "critical activity" for clarity and flexibility by removing amorphous "critical activity" qualifying terms like "significant investment" and "significant bank function" and, instead, focusing on variable risk-based characteristics. The Federal Banking Agencies incorporated concepts from OCC FAQs 7, 8, and 9 into the Final Third-Party Guidance, noting that banking organizations my assign criticality either by relationship or by activity so long as a sound methodology is utilized.
- Reiterating that the Final Third-Party Guidance is relevant to all banking organizations, including community banks, and incorporating concepts from FAQs 5, 6, 7, and 9.
- Emphasizing that the Final Third-Party Guidance adopts a principles-based approach to risk management rather than a more rigid prescriptive approach, including by noting that certain traditional banking arrangements (*e.g.*, relationships with customers) may, when viewed through a principles-based approach, be altered significantly and in novel ways where the customer is a fintech or other type of entity that presents enhanced risks that merit a commensurate increase in risk management processes.
- On diligence, the Federal Banking Agencies restate that third-party relationships vary by risk and scope and that not all relationships require the same level of diligence and risk management oversight; however, the agencies specifically declined to categorically place certain types of third-party relationships in either a reduced or heightened diligence and risk category. Further, noting that many banking organizations may beneficially utilize third parties to supplement their diligence or information gathering efforts, the Federal Banking Agencies emphasize that such collaborative efforts do not abrogate the responsibility of the banking organization to manage its third-party relationships in a safe and sound manner.
- The Final Third-Party Guidance removes the term "critical subcontractor" and instead restates and clarifies that all third-party activities should be evaluated based on the potential risk to the banking organization, and banking organizations should evaluate if, how, and to what extent a third-party's use of subcontractors adds additional risks to the banking organization.
- The Federal Banking Agencies also incorporated concepts from OCC FAQs 6 and

26, clarifying that oversight and accountability should occur organically throughout the risk management life cycle.

- The Final Third-Party Guidance also further distinguishes between board and management responsibilities "to avoid the appearance of a prescriptive approach to the board's role in the risk management life cycle, while still emphasizing that the board has ultimate oversight responsibility to ensure that the banking organization operates in a safe and sound manner and in compliance with applicable laws and regulations."[13]

You can access the Final Third-Party Guidance here: https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management#citation-6-p37921.

CFPB Report Reviews Financial Institution Use of Chatbot Technology

On June 6, 2023, the CFPB published an issue spotlight report on financial institutions' increasing use of artificial intelligence for customer service and the risks this presents to consumer financial services (the "Chatbot Technology Report").[14] The CFPB notes in the Chatbot Technology Report that financial institutions are increasing their use of technologies in customer service that simulate human-like responses with computer programming—commonly referred to as "chatbots." According to the report, each of the 10 largest commercial banks in the U.S. have used chatbots to interact with customers.[15] The CFPB reports that approximately 37% of the U.S. population interacted with a bank's chatbot technology in 2022, and more people are expected to make these interactions as banks shift to implement more sophisticated technologies.[16]

Financial institutions utilize chatbots for cost efficiencies and to provide consumers with more immediate answers to common questions; however, the Chatbot Technology Report notes that chatbot technology may not be able to solve a consumer's complex or novel problems. Chatbots can struggle to recognize or resolve a consumer's concern or dispute since chatbots are limited to system information that does not allow for further research or more flexible responses that are outside of the technology's data inputs.

The Chatbot Technology Report also highlights the risks posed by the use of chatbots. First, the CFPB highlights that financial institutions can risk noncompliance with consumer financial protection laws by using chatbot technology if chatbots are unable to recognize when consumers are invoking rights under federal law, and chatbots can fall short of data and privacy protection standards. Second, with chatbot use, financial institutions risk the trust that consumers have with these institutions as consumers may continually be unable to receive meaningful help from the technology. Lastly, financial institutions risk harm to consumers if chatbot technology provides incorrect or insufficient information that is based on unreliable data and consumers rely on this faulty information as true.

You can access the Chatbot Technology Report here: https://www.consumerfinance.gov/d

ata-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/.

CFPB Publishes Spring Rulemaking Agenda, including Increased Regulatory Reach over Non-Bank Entities

On June 13, 2023, the Office of Information and Regulatory Affairs released the Spring 2022 Unified Agenda of Regulatory and Deregulatory Actions (the "Rulemaking Agenda"),[17] which includes contributions from the CFPB setting forth the matters the CFPB reasonably anticipates having under consideration during the period from June 1, 2023, to May 31, 2024.[18] There are seven items on the CFPB's agenda in the Pre- or Proposed Rule Stage, including: (i) overdraft fee rulemaking, (ii) fair credit reporting act rulemaking, (iii) rulemaking regarding fees for insufficient funds, (iv) required rulemaking on personal financial data rights, (v) amendments to FIREA concerning automated valuation models, (vi) property assessed clean energy financing rulemaking, and (vii) a new addition to the Rulemaking Agenda related to the supervision of larger participants in consumer payment markets (the "Larger Participants Rule").[19]

Section 1024 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") granted the CFPB the authority to exercise supervision over certain covered nonbank entities—those considered "larger participants" in certain markets—for compliance with federal consumer financial laws.[20] According to the abstract for the proposed Larger Participants Rule, the CFPB plans to use its authority under Section 1024 to define larger participants in markets for consumer payments.

You can access the CFPB's Spring Rulemaking Agenda here: https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3170&csrf_token=ED8211BCD3D1ED5A4184195F471119BD0F45484413043A52E1C57E4350B792C576C0DC108CC3BCDB1E73F275BD1093D467CC.

CISA to Propose New Ransomware Payment Reporting Rule

On June 13, 2023, the Cybersecurity and Infrastructure Security Agency ("CISA"), an agency of the Department of Homeland Security ("DHS"), announced in the Rulemaking Agenda its expectation to propose new rules to implement the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). CIRCIA requires "covered entities" (i) to report "significant cyber incidents" to CISA not later than 72 hours after the covered entity reasonably believes that the incident has occurred, and (ii) to report the payment of ransoms related to cyber incidents not later than 24 hours after the payment has been made, pursuant to rules that must be proposed by the Director of CISA by March 2024.[21] CIRCIA defines "covered entities" as entities in the critical infrastructure sector[22] that satisfy the further definition to be provided in the forthcoming rules.

You can read the abstract of the proposed rule in the Rulemaking Agenda here: https://www.r

eginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1670-AA04.

CFPB, HHS, and Treasury Issue Request for Information on Medical Payment Products

On July 12, 2023, the CFPB, the United States Department of Health and Human Services ("HHS"), and the United States Department of Treasury ("Treasury") published a request for information regarding medical payment products (the "Medical Payments RFI").[23] The Medical Payments RFI requests information from interested parties on "medical credit cards, loans, and other financial products used to pay for health care."[24] According to the Medical Payments RFI, the CFPB, HHS, and Treasury seek to understand how "these products may allow health care providers to operate outside of a broad range of patient and consumer protections" and "whether these products may contribute to health care cost inflation, displace hospitals' provision of financial assistance, lead patients to pay inaccurate or inflated medical bills, increase the amount patients must pay due to financing costs, or otherwise harm patients' mental, physical, and financial well-being, including through downstream credit reporting and debt collection practices."[25]

The Medical Payments RFI poses a series of market-level questions, questions posed to individuals, and CFPB, HHS, and Treasury specific questions. According to the CFPB, responses to the Medical Payments RFI will be used to shape policy options to protect consumers of medical services.

You can access the Medical Payments RFI here: https://www.federalregister.gov/documents/2023/07/12/2023-14726/request-for-information-regarding-medical-payment-products.

Federal Reserve Publishes Master Accounts and Services Database

On June 16, 2023, the Board of Governors of the Federal Reserve System (the "Board") published a new Master Account and Services Database (the "Master Account Database") that provides public access to a searchable database of financial institutions that have requested access to Federal Reserve master accounts and financial services ("Master Accounts"). The Master Account Database has two components: an existing Master Accounts database; and a requested Master Accounts database.[26] The Board will update each database on a quarterly basis.[27]

You can access the Master Account Database here: https://www.federalreserve.gov/paymentsystems/master-account-and-services-database-about.htm.

LITIGATION AND ENFORCEMENT DEVELOPMENTS

FTC Issues Final Order Requiring Mastercard to Stop Blocking Competing Debit Card Payment Networks in Tokenized Transactions

On May 30, 2023, the Federal Trade Commission (the "FTC") finalized a consent order (the "FTC Final Order")[28] with Mastercard Incorporated ("Mastercard") enjoining Mastercard from using debit card tokenization practices to violate the Durbin Amendment to the

Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and its implementing regulation, Regulation II (collectively referred to herein as the "Durbin Amendment").[29] The FTC Final Order mirrors the proposed order into which the FTC and Mastercard conditionally entered on December 23, 2022, as part of the initial consent agreement addressing the issue. In the FTC's complaint against Mastercard (the "FTC Complaint"), the FTC alleged that Mastercard unlawfully suppressed competition in violation of the Durbin Amendment by preventing merchants from being able to route card not present transactions initiated using debit cards tokenized by Mastercard to alternative payment card networks.[30]

The Durbin Amendment, in relevant part, prohibits payment card network exclusivity with respect to debit cards (including tokens) by: (i) prohibiting debit card issuers and payment card networks from directly or indirectly limiting the number of networks on which a debit transaction can be processed to less than two unaffiliated networks, (ii) requiring debit card issuers to enable at least two unaffiliated networks on each debit card, and (iii) prohibiting payment card networks from limiting an issuer's ability to contract with any other network.[31] Additionally, the Durbin Amendment prohibits an issuer or payment card network from "inhibiting a merchant's ability to choose which network enabled for the debit card is used to process a given transaction."[32]

Mastercard network rules require that debit card primary account numbers (the "PANs") must be tokenized before they may be loaded into "ewallets" such as Apple Pay, Google Pay, and Samsung Wallet.[33] Virtually all tokenization services necessary for meeting this requirement with respect to Mastercard debit cards are performed by Mastercard. In order for a payment transaction initiated with a token to be processed by a payment card network, the payment token must be "detokenized" whereby the token used to initiate the transaction is converted back to the debit card PAN. As the provider of tokenization services for debit cards issued on its network, Mastercard maintains a "token vault" that contains both debit card users' tokens and their corresponding PANs, and access to this token vault is necessary for detokenization and transaction processing.

In the FTC Complaint, the FTC alleged that Mastercard violated the Durbin Amendment by refusing to detokenize card not present (ecommerce) transactions for routing to and processing by non-Mastercard networks.[34] According to the FTC, Mastercard's refusal to detokenize ecommerce transactions for other networks forced "card-not-present ewallet transactions made with Mastercard-branded debit cards to Mastercard . . . to the detriment of competing . . . networks, merchants, and ultimately consumers."[35] The FTC Complaint alleged that this practice by Mastercard violates the Durbin Amendment by inhibiting merchants' ability to route ewallet ecommerce transactions to any network enabled on the debit card.

While Mastercard does not concede that any of its actions detailed in the FTC Complaint violated the Durbin Amendment, the FTC Final Order requires Mastercard to provide competing networks with the customers' PANs to detokenize ewallet card-not-present transac-

tions when such networks receive tokens to process debit card payments.[36] The FTC Final Order also bans Mastercard from taking any action to prevent competitors from providing their own payment token service or offering tokens on Mastercard-branded debit cards.[37]

You can access the FTC Complaint and FTC Order here: https://www.ftc.gov/system/files/ftc_gov/pdf/2010011C4795MastercardDurbinOrder.pdf.

PayPal Files New Motion to Challenge CFPB Prepaid Accounts Short-Form Fee Disclosure Rule

On May 26, 2023, PayPal Inc. ("PayPal") filed a motion to renew its challenge to the short-form disclosure requirements of the regulations related to prepaid accounts (the "Prepaid Rule") promulgated by the CFPB as part of Regulation E.[38] The CFPB also filed a motion disputing PayPal's claims and requesting summary judgement.[39]

In 2020, PayPal sued the CFPB, challenging the short-form disclosure requirements of the Prepaid Rule on statutory, administrative, and constitutional grounds. The United States District Court for the District of Columbia (the "DC District Court") did not rule on PayPal's administrative and constitutional claims because it held that PayPal succeeded in its statutory claim that the Prepaid Rule's short-form disclosure requirements exceeded the CFPB's authority under the Electronic Fund Transfer Act ("EFTA").[40] Specifically, the DC District Court agreed with PayPal's claim that the CFPB had made mandatory the use of a short-form model clause under the Prepaid Rule while the EFTA did not authorize the CFPB to issue mandatory model clauses that dictate form, structure and content.[41] The DC District Court concluded that the CFPB is only permitted under the EFTA to offer *optional* model forms and clauses.[42] However, on February 3, 2023, the United States Court of Appeals for the District of Columbia (the "DC Circuit") overturned the DC District Court's ruling, finding that the Prepaid Rule did not mandate the use of model clauses as part of the short-form disclosure requirements.[43] The DC Circuit Court determined that the CFPB's short-form disclosure model clause was not a "mandatory model clause" because the CFPB did not require the use of specific, copiable language from the model form and remanded the case to the DC District Court for rulings on PayPal's constitutional and administrative claims.[44]

In its new motion, PayPal requests summary judgment arguing that the Prepaid Rule's short-form disclosure requirements violate PayPal's First Amendment rights and that the CFPB violated the Administrative Procedure Act when it implemented the rule in 2019.

Specifically, PayPal argues that the short-form disclosure requirement violates PayPal's First Amendment rights because it imposes limitations on PayPal's commercial speech without the CFPB having shown that the mandated Prepaid Rule language is both reasonably related to the CFPB's interest in preventing the deception of consumers and not unjustified or unduly burdensome (the standard for restricting commercial speech).[45] PayPal argues that the CFPB's requirements do not meet those standards and in fact, force PayPal to make

statements likely to confuse and mislead consumers while also prohibiting the company from clearing up the resulting confusion.[46] In its own motion, the CFPB disputes those claims and asserts that laws which compel commercial speech are subject to more lenient standards and only need to be reasonably related to a government interest and not unduly burdensome.[47]

In support of its administrative claims, PayPal argues that the CFPB failed to perform an appropriate cost-benefit analysis when it applied the Prepaid Rule's short-form disclosure requirements to digital wallets and that the requirements as applied to digital wallets are arbitrary and capricious.[48] Under the Administrative Procedure Act ("APA"), the CFPB is required to consider the costs and benefits of all regulations it proposes. PayPal argues that the CFPB's considerations of the costs and benefits of the Prepaid Rule as applied to prepaid products like General Purpose Reloadable Cards cannot apply to digital wallets and a separate analysis would have to be undertaken.[49] In their corresponding motion, the CFPB contends that while digital wallets were not a major focus of their cost-benefit analysis, such applications were considered thoroughly.

The case before the DC Circuit is *PayPal Inc. v. CFPB,* No. 21-5057. You can access the docket here: https://ecf.dcd.uscourts.gov/cgi-bin/DktRpt.pl?213550.

Putative Class Sues Walmart Over Fraudulent Money Transfers Facilitation

On June 9, 2023, a putative class of plaintiffs (the "Walmart Plaintiffs") filed suit against Walmart, Inc. ("Walmart") alleging that Walmart failed to take timely and effective measures to detect and prevent fraud in connection with the processing of money transfers originated at its store locations, allowing fraudsters to perpetrate their schemes on unsuspecting Walmart customers.[50] The suit adopts the same general factual allegations brought by the FTC against Walmart in its suit against the company for violations of the Federal Trade Commission Act.

In addition to its typical retail services, Walmart provides financial services to consumers, including money transfers, credit cards, reloadable debit cards, check cashing, and bill payments and acts as an agent for multiple money transfer services, including MoneyGram, Ria and Western Union.[51] The FTC has alleged, and now the Walmart Plaintiffs allege, that Walmart failed to address the risk of fraudulent transfers arising from its provision of these services despite being aware of telemarketing and other mass marketing frauds that direct consumers to utilize Walmart's money transfer services. Further, the FTC has alleged, and now the Walmart Plaintiffs allege, that Walmart failed to comply with two prior court orders obtained by the FTC against Walmart requiring, among other things, the establishment of comprehensive anti-fraud programs covering employee training, consumer warnings, and reasonable detection and investigation protocols. Walmart's failure to interdict the fraudsters has, according to the Walmart Plaintiffs, resulted in substantial injury to the Walmart Plaintiffs.

The named plaintiff in the case was duped by a scheme in which fraudsters promised to pay

her $700 per month to place an advertisement on her vehicle. She was then overpaid for the first month of service in the amount of $5,200. When the fraudsters called to confirm that she received the check, she was directed to deposit the check, but to send back $4,500 to correct the overpayment using Walmart's money order services. The check bounced, but the money order was gone.

The Walmart Plaintiffs accuse Walmart of (i) breach of the covenant of good faith and fair dealing, (ii) violations of Illinois' Consumer Fraud and Deceptive Business Practices Act, and (iii) violations of the EFTA. The Walmart Plaintiff's EFTA claim rests on the assertion that the funds transfers were unauthorized.

The case before the Northern District of Illinois is *Ayala-Bland v. Walmart, Inc.*, No. 1:23-cv-03650. You access the docket report here: https://ecf.ilnd.uscourts.gov/cgi-bin/DktRpt.pl?434363.

Wyoming District Court Denies Wyoming's Motion to Intervene in Custodia's Master Account Dispute

On May 17, 2023, the United States District Court for the District of Wyoming (the "Wyoming District Court") denied the state of Wyoming's motion to intervene (the "Intervention Motion") in the ongoing case between Custodia Bank, Inc. ("Custodia") and the Board and the Federal Reserve Bank of Kansas City (the "FRBKC," together the "Defendants").[52] The Wyoming District Court summarized the central issue in Custodia's case as being whether "Defendants have a non-discretionary duty to grant" Custodia's application for a Federal Reserve master account (a "Master Account").[53]

Custodia organized as a Wyoming state-chartered special purpose depository institution ("SPDI") with the intent of providing a limited set of banking services focused on payment services and crypto-asset custody.[54] Thereafter Custodia applied to the Board for membership in the Federal Reserve System and to the FRBKC for a Master Account. Custodia alleges that the Board, in coordination with the White House, intervened in Custodia's application with the FRBKC for a Master Account, directed the denial of the Master Account application, and denied Custodia's membership in the Federal Reserve System, in a broad and coordinated effort to restrict the expansion of crypto-asset related products and services in the banking industry for state-chartered institutions. On March 24, 2023, the Board released the full text of its order, dated January 27, 2023, denying Custodia's application for membership in the Federal Reserve System (the "Membership Order").[55] The Board's release of the full text of the Membership Order followed Custodia's filing of an amended complaint on February 28, 2023 (the "Amended Complaint")[56] in the case. In the Membership Order, the Board expounded on its reasons for denying Custodia Federal Reserve membership, including, in part, concerns over the "untested nature" of Wyoming's SPDI regulatory regime.

The Attorney General of the State of Wyoming filed the Intervention Motion on April 13, 2023, noting that the "tenor of the dispute . . . appears to include, in part, a debate over Wyoming's regulation of [SPDIs]" and arguing that "to the extent that [the Board's and the FRBKC's] decisions and interpretations of federal law, and Wyoming's SPDI statutes and

regulations, question or challenge Wyoming's legal framework, the Attorney General is seeking leave to intervene in the defense of that framework."[57]

In its order denying the Intervention Motion, the Wyoming District Court stated that allowing Wyoming to intervene "would unnecessarily expand this case from statutory construction to one that involves what the Defendants are allowed to consider and further analysis into the sufficiency of Wyoming's statutory framework."[58] Specifically, the Wyoming District Court held that the court need only analyze whether the Defendants had a mandatory duty to grant Custodia a Master Account and that allowing Wyoming to intervene would unnecessarily force the court to "delve into any collateral issues such as the sufficiency of the Wyoming legal framework or the dual banking system as a whole."[59]

Furthermore, the Wyoming District Court held that Wyoming failed to assert a valid claim for relief. Wyoming asserted in its Intervention Motion that the Defendants "violated 12 U.S.C.A. § 248a(c)(2) [by] acting inequitable toward Wyoming SPDI Banks;"[60] however, the Wyoming District Court held that Section 248a does not provide plaintiffs with a claim for inequitable treatment and no other basis for jurisdiction exists for the court to preside over a claim premised on 248a.[61]

While the Wyoming District Court denied Wyoming's Intervention Motion, it specifically noted that Wyoming has already and may continue to supplement or file an amended amicus brief addressing the new issues in which it argues it has an interest.[62]

On June 8, 2023, the Wyoming District Court granted the Defendants' motion to dismiss solely with respect to Custodia's Mandamus Act claim against the Board, holding that relief under the Mandamus Act is unavailable because the APA provides an adequate remedy. The court denied the remainder of the Defendants' motion to dismiss with respect to all other claims.

The case before the United States District Court for the District of Wyoming is *Custodia Bank, Inc. v. Federal Reserve Board of Governors et al.*, No. 22-CV-00125. You can access the docket here: https://ecf.wyd.uscourts.gov/cgi-bin/DktRpt.pl?61107.

PayServices Bank Sues San Francisco Federal Reserve Bank Over Master Account Denial

On June 27, 2023, PayServices Bank ("PayServices") filed a complaint (the "PayServices Complaint") against the Federal Reserve Bank of San Francisco ("FRBSF") over the FRBSF's denial of its application for a Master Account.[63]

PayServices, a provisionally approved Idaho state-chartered bank, proposes to be a non-lending bank focused on facilitating payments related to the international trade of commodities for small to medium sized enterprises. According to the PayServices Complaint, the bank would release transaction funds only after its process and technology solution confirmed that the physical commodities had been verified by governmental customs agencies. According to the PayServices Complaint, the FRBSF denied PayServices' application for a Master Account because the bank's line of business is novel,

unproven, and presents an undue risk to the FRBSF. PayServices argues that its business model is not novel, but simply focused on specialized transactions and, further, that any risk to the FRBSF is negligible because PayServices does not offer credit products, does not allow negative account balances, and only processes payment transactions upon the delivery of goods and verification by customs agents.[64]

PayServices argues that the Depository Institutions Deregulation and Monetary Control Act (DIDMCA) mandates that "[a]ll Federal Reserve bank services . . . shall be available to nonmember depository institutions" and thus the FRBSF had a nondiscretionary duty to issue PayServices a Master Account.[65] PayServices seeks relief under the APA arguing that the FRBSF is an "agency" within the meaning of the APA because it exercises substantial delegated authority from the Board and is subject to supervision by the Board, which is itself an "agency" subject to the APA's judicial review provisions.[66] PayServices also seeks relieve under the Mandamus Act arguing that the President of the FRBSF is an officer of the United States, and the Due Process Clause of the Fifth Amendment to the U.S. Constitution arguing that PayServices has a protectible property interest in a Master Account which it was deprived of without procedural and substantive due process.[67]

The case before the United States District Court for the District of Idaho is *PayServices Bank v. Federal Reserve Bank of San Francisco*, No. 1:23-cv-00305. You can access the docket here: https://ecf.idd.uscourts.gov/cgi-bin/DktRpt.pl?52494.

FTC Files Amended Complaint in Walmart Fraudulent Money Transfers Facilitation Case

On June 30, 2023, the FTC filed an amended complaint (the "Amended FTC Complaint") in the United States District Court for the Northern District of Illinois against Walmart, Inc. ("Walmart") for its alleged failure to take timely and effective measures to detect and prevent fraud in connection with the processing of money transfers originated at its store locations, allowing fraudsters to perpetrate their schemes on Walmart customers.[68] Specifically, the Amended FTC Complaint augments a previous complaint filed by the FTC in June 2022 alleging violations of the FTC Act and the Telemarketing Sales Rule ("TSR").

The court previously dismissed, without prejudice, the FTC's allegation that Walmart violated the TSR by failing to address the risk of fraudulent cash-to-cash money transfers ("Fraudulent Transfer Risk") arising from its provision of money transfer services despite being aware of telemarketing and other mass marketing frauds that direct consumers to utilize Walmart's money transfer services.[69] In the Amended FTC Complaint, the FTC provides the court with additional arguments responding to the court's dismissal of its allegation that Walmart violated the TSR (the "TSR Allegation Dismissal").

The FTC claims that Walmart violated the TSR by failing to address the Fraudulent Transfer Risk, thereby providing "substantial assistance or support" to the telemarketers who commonly induced consumers to pay for goods or services through the use of false or misleading

statements and accepted cash-to-cash money transfers as payments for goods or services offered through telemarketing.[70]

The TSR Allegation Dismissal stated that the FTC's TSR allegations against Walmart failed because the FTC neither plead facts sufficient to establish an underlying violation of the TSR as to which Walmart provided substantial assistance nor plead facts sufficient to establish that Walmart knew, or consciously avoided knowing, of such schemes thereby providing substantial assistance to the fraudsters.[71]

The TSR bans the use of cash-to-cash money transfers in all telemarketing transactions,[72] and in the Amended FTC Compliant, the FTC alleged that the following facts show that Walmart provided substantial assistance to fraudsters:

i. Between 414-1,400 Walmart employees needed training to help them identify fraud and suspicious activity,[73] and Walmart's failure to provide such training "allowed employees to become complicit in the frauds";[74]

ii. Despite receiving notice of practices that the FTC expects money transferers to take when processing cash-to-cash transactions, Walmart failed to implement changes to its practices until years following receipt of the notice;[75]

iii. Walmart's money transfer partners have suspended Walmart from processing orders on multiple occasions for Walmart's noncompliance with their internal policies, which comply with the TSR;[76]

iv. Walmart knew of the high potential for fraud and failed to properly warn consumers by posting warning signs or issuing brochures or pamphlets about consumer fraud;[77]

v. Walmart failed to prevent transfers exhibiting traits characteristic of fraud, such as high dollar amounts, back-to-back transfers, transfers to high-risk countries known for fraud, transfers between senders and receivers with no apparent relationship, transfers fitting the pattern of known money transfer scams, consumers switching between money transfer systems, and transfers involving first-time senders;[78] and

vi. Walmart has consciously avoiding knowing about its own employees' involvement in fraudulent cash-to-cash money transactions.[79]

The FTC is seeking a permanent injunction to prevent future violations of the FTC Act and TSR by Walmart in connection with money transfers.

The case before the U.S. District Court for the Northern District of Illinois is *Federal Trade Commission v. Walmart Inc.,* Case No. 1:22-cv-3372. You can access the docket here: https://ecf.ilnd.uscourts.gov/cgi-bin/DktRpt.pl?416367.

ENDNOTES:

[1]*Analysis of Deposit Insurance Coverage*

on Funds Stored Through Payment Apps, CFPB (Jun. 1, 2023), https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/full-report/.

[2]*Id.*

[3]*Id.*

[4]*Id.*

[5]*Id.*

[6]*Consumer advisory: Your money is at greater risk when you hold is in a payment app, instead of moving it to an account with deposit insurance*, CFPB (Jun. 1, 2023), https://www.consumerfinance.gov/about-us/newsroom/consumer-advisory-your-money-is-at-greater-risk-when-you-hold-it-in-a-payment-app-instead-of-moving-it-to-an-account-with-deposit-insurance/.

[7]*Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37,920 (Jun. 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management#citation-6-p37921.

[8]*Proposed Interagency Guidance on Third-Party Relationships: Risk Management*, 86 Fed. Reg. 38,182 (Jul. 19, 2021), https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.

[9]OCC Bulletin 2013-29.

[10]Final Third-Party Guidance *supra* note 7 at 37,920.

[11]Proposed Third-Party Guidance *supra* note 8.

[12]Final Third-Party Guidance *supra* note 7 at 37,921.

[13]*Id.* at 37,921 - 37,927.

[14]*Chatbots in Consumer Finance*, CFPB (Jun. 6, 2023), https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/.

[15]*Id.*

[16]*Id.*

[17]*Spring 2023 Unified Agenda of Regulatory and Deregulatory Actions*, Office of Information and Regulatory Affairs, Office of Management and Budget (Jun. 13, 2023), https://www.reginfo.gov/public/do/eAgendaMain.

[18]*Semiannual Regulatory Agenda*—Preamble, CFPB (Jun. 13, 2023), https://www.reginfo.gov/public/jsp/eAgenda/StaticContent/202304/Preamble_3170_CFPB.pdf.

[19]Agency Rule List—Spring 2023, CFPB (Jun. 13, 2023), https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3170&csrf_token=ED8211BCD3D1ED5A4184195F471119BD0F45484413043A52E1C57E4350B792C576C0DC108CC3BCDB1E73F275BD1093D467CC.

[20]12 U.S.C.A. § 5514(a)(1)(B).

[21]H.R. 2471 Consolidated Appropriations Act, 2022, https://www.congress.gov/117/bills/hr2471/BILLS-117hr2471enr.pdf at 996.

[22]Critical infrastructure sector refers to the critical infrastructure designated pursuant to Presidential Policy Directive 2—Critical Infrastructure Security and Resilience ("PPD-21"), which designates Treasury as the sector-specific agency for designating critical financial services. PPD-21 was issued February 12, 2013 and is available here: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[23]CFPB, HHS, and Treasury, *Request for Information Regarding Medical Payment Products*, 88 Fed. Reg. 44,281 (Jul. 12, 2023), https://www.federalregister.gov/documents/2023/07/12/2023-14726/request-for-information-regarding-medical-payment-products.

[24]*Id.*

[25]*Id.*

[26]Federal Reserve, *Federal Reserve Board Publishes a Database of Financial Institutions with Access to, or Requests to Access, Federal Reserve Bank Master Accounts and Services* (Jun. 16, 2023), https://www.federalreserve.gov/newsevents/pressreleases/other20230616a.htm.

[27]*Id*.

[28]*In the Matter of: Mastercard Incorporated*, C-4795 (FTC May 30, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2010011C4795MastercardDurbinOrder.pdf.

[29]The Durbin Amendment, enacted as Section 1075 of the Dodd-Frank Act and implemented through Federal Reserve Board Regulation II, limits the amount of interchange fees that larger debit card issuers can charge or receive on debit card transactions. 15 U.S.C.A. § 1693 0-2; 12 CFR Part 235.

[30]*In the Matter of: Mastercard Incorporated*, (FTC Dec. 23, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2010011mastercardcomplaint.pdf.

[31]FTC Final Order *supra* note 28 at 4.

[32]*Id*.

[33]*Id.* at 5.

[34]*Id.* at 7.

[35]*Id.* at 8.

[36]FTC Final Order *supra* note 28 at 1.

[37]*Id.*

[38]*PayPal Inc. v. CFPB,* No. 1:19-cv-03700, Doc. 39 (D.D.C. May 26, 2023).

[39]*PayPal Inc. v. CFPB,* No. 1:19-cv-03700, Doc. 38 (D.D.C. May 26, 2023).

[40]*PayPal Inc. v. CFPB*, No. 1:19-cv-03700, Doc. 27 (D.D.C. Dec. 30, 2020).

[41]*Id*.

[42]15 U.S.C.A. § 1693(b).

[43]*PayPal Inc. v. CFPB et al.*, No. 21-5057, Doc. 1984449 (D.C. Feb. 3, 2023).

[44]*PayPal Inc. v. CFPB supra* note 40 at 2.

[45]*PayPal Inc. v. CFPB supra* note 38 at 35.

[46]*Id.*

[47]*PayPal Inc. v. CFPB supra* note 39 at 32.

[48]*PayPal Inc. v. CFPB supra* note 38 at 28.

[49]*Id.* at 29.

[50]*Ayala-Bland v. Walmart, Inc.*, No. 1:23-cv-03650, Doc. 1 (N.D. Ill. Jun. 9, 2023), https://ecf.ilnd.uscourts.gov/cgi-bin/DktRpt.pl?434363.

[51]*Id*. at 2.

[52]*Custodia Bank, Inc. v. Federal Reserve Board of Governors et al.*, No. 22-CV-00125, Doc. 162 (D. Wyo. May 17, 2023).

[53]*Id.* at 2.

[54]*Custodia Bank, Inc. v. Federal Reserve Board of Governors et al.*, No. 22-CV-00125, Doc. 121 at 2 (D. Wyo. Feb. 28, 2023)

[55]FRB Order No. 2023-02: Custodia Bank, Inc.—Order Denying Application for Membership (Jan. 27, 2023), https://www.federalreserve.gov/newsevents/pressreleases/files/orders20230324a1.pdf.

[56]*Custodia Bank, Inc. v. Federal Reserve Board of Governors et al.*, No. 22-CV-00125, Doc. 121 (D. Wyo. Feb. 28, 2023).

[57]*Custodia Bank, Inc. v. Federal Reserve Board of Governors et al.*, No. 22-CV-00125, Doc. 140 (D. Wyo. Apr. 13, 2023).

[58]*Custodia Bank, Inc. v. Federal Reserve Board of Governors et al. supra* note 52 at 5.

[59]*Id.* at 5.

[60]*Id.* at 5-6.

[61]*Id.* at 7.

[62]*Id.*

[63]*PayServices Bank v. Federal Reserve Bank of San Francisco*, No. 1:23-cv-00305, Doc. 1 (D. Idaho Jun. 27, 2023).

[64]*Id*. at 10-12.

[65]*Id*. at 16.

[66]*Id*. at 18-22.

[67]*Id*. at 22-24.

[68]*Fed. Trade Comm'n v. Walmart Inc.*, Case no. 1:22-cv-03372, Doc. 62 (N.D. Ill. Jun. 30, 2023), https://ecf.ilnd.uscourts.gov/cgi-bin/DktRpt.pl?416367.

[69]*Fed. Trade Comm'n v. Walmart Inc.*, Case no. 1:22-cv-03372, Doc. 52 (N.D. Ill. March 27, 2023), https://ecf.ilnd.uscourts.gov/cgi-bin/DktRpt.pl?416367.

[70]*Id.* at 20.

[71]16 CFR 310.3(b); *Id.* at 22.

[72]Amended FTC Complaint *supra* note 68 at 56.

[73]*Id.* at 46.

[74]*Id.*

[75]*Id.* at 57-58.

[76]*Id.* at 51-53.

[77]*Id.* at 53-54, 61.

[78]*Id.* at 60-61, 64, 67-68, 71, 75, 78.

[79]*Id.* at 62-63.

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.