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

September/October 2021 ▪ Volume 24 ▪ Issue 5

FINTECH INTERVIEW: WHAT CAN WE LEARN FROM THE GAMERS? QUITE A LOT

Stephen Mathai-Davis is the co-founder and CEO of Q.ai, an artificial intelligence-powered robo-investing platform. In late August, ***FinTech Law Report*** *interviewed Mathai-Davis to see what his company is doing in the investing space and his thoughts as to the gamification of investing and the growth of AI, among other topics.*

FinTech Law Report*: What is it that Q.ai does, presently?*

Stephen Mathai-Davis: We're bringing institutional investing to individual investors and, by so, empowering them. We're trying to help users to express themselves in investments. I used to work in the sell side and, there, the funds are the expressions of their managers, in a way. But if you're an individual investor, you don't get access to a lot of that stuff. You only get access to things that a particular asset management company built. We want to empower folks to really create their own investment experiences.

By that I mean: We call our products "investment kits," and it's all structured through an [separately managed account] SMA, so we're not selling funds. We're selling the whole idea of buying into different kits that are powered by our AI strategies—kits that give you different exposures to different time horizons, different themes, and different risk levels.

FinTech*: What are some examples of this?*

Mathai-Davis: We have our signature kits, which offer long-term focused strategies, whether it's value strategy, emerging tech, factor rotation, macro global trends. And we have our limited-

IN THIS ISSUE:

THOMSON REUTERS®

42689668

edition kits, which tend to be the shorter-term focused trades. We put together a Back to School kit in August, which gives you a dynamically managed trade basket. If you wanted to make that play, traditionally, maybe you go buy Target or Amazon. I would respectfully say: That's not the way to do it. The way to do it is to buy a dynamically managed basket that's trading all the key retailers: the Foot Lockers, the BJ's, the Kohl's.

For those who have access, the high net worth individuals, they'll get pitched something like this. Structured product desks usually create these types of products and sell them to the buy side. We've brought this directly to the user. We're dynamically managing risk. So we also have a Summer Fund because people were going out this summer, and it includes cruise lines, casinos, hotels, rentals and gas stations. And we released a global microchip shortage play, based on what's going on with semiconductors. There are issues with supply as demand is increasing rapidly. Especially with smart cars. The smart products market is driving massive demand. So imagine if you could play the global microchip shortage.

We have something we call "Meme Stock Frenzy," which gives you the ability to play the top stocks from Wall Street Bets on Reddit. We've created a strategy using an advanced form of NLP [natural language processing]. You can get the top-mentioned stocks that have the best sentiment on Reddit, and you can buy a basket of that. We're also releasing "Guilty Pleasures," a "vice portfolio" that's sort of the anti-ESG: tobacco, cannabis, booze. Think of it as the perfect goldilocks barbell strategy where you've got a few cash-full companies, some with current hypergrowth and, in the middle, you have a really steady growth. And we have a Precious Metals kit. People can play gold, platinum, palladium. silver. Again, these are not ETFs. We're dynamically managing the risk we're trading within each kit. We do dynamic asset allocation between them.

FinTech: *What type of audience are you aiming for?*

Mathai-Davis: We're trying to relate to the Millennial/Generation Z investor who is looking for something different. If you're making over, say, $125,000 today, and maybe you have

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

One Year Subscription ● 6 Issues ● $ 1020.00

$75,000 invested, you don't have a lot of options. If you've got less than $1,000, you have a *plethora* of options. There are tons of micro platforms. But if you even have $20,000, you don't have a lot of options. [Typical] robo-investing is really just old school wealth management with a digital wrapper. It's not investment management.

We're trying to reimagine what the buy side does for people. We've released AI-powered hedging. When I was running funds, I was asked to put on dynamic hedges, and, for the really good funds, it's mostly systemized. You're not manually doing it; you're not listing hedges left and right. With our downside protection, you can elect to go into [a kit], and then we're throwing on hedges, maybe moving you into cash because we're worried the market is going too down. Rather than trying to short the market for you, we just put you into cash, or we're buying a long ETF that gives you short exposure.

If you're a super high-net-worth individual, you have access to all this. I'd be trading options, doing futures, dynamic stock picks in the consumer tech space. I was doing things that, when I spoke to my friends, nobody had access to. So I think AI and advancements in quantitatively heuristics and technology has really made it easier.

***FinTech**: What's your timeframe been?*

Mathai-Davis: We've been working on this for over five years. We spent years developing our investment tech, some of which I was originally using to run money for other people. Now we're trying to productize it in a way that makes it really simple and easy. The product itself, the mobile app, is still in beta. We launched in March, and then we went product to product [after] the launch date.

We're just trying to make it easy. That's the primary thing. I've spent my life in the investing business. When I was a kid who was exposed to stock trading and investing at nine years old by my dad. I'm a CFA, I've been a trader, a portfolio manager, an analyst, and with some of the apps out there, I had trouble understanding them! So the average person may have no idea what they're doing. For us, when you come on our dashboard, the first thing you're told is: Here's how you're doing, here's the return, here's how your balance has changed. We also show your personal rate of return, how you're doing for yourself. And then, "Here are the different kits you're currently in." Am I using the AI-powered allocation? Am I not using it, what other kits can I go in, what's going to be released soon? Think of it this way, we are bringing the Tesla and Apple customer experience to investment management.

***FinTech**: What regulatory issues are these changes creating? I'm thinking of the SEC's public comments of late on "gamification" of stocks—what sort of new fintech-related rules could be coming in the next few years, and how can brokers and investors adapt?*

Mathai-Davis: The biggest problem with a lot of the apps is their idea of artificial scarcity—you have to do something or else someone else will get something. They're trying to create extrinsic incentives, which desensitizes you

to potential risks. That's not really investing. For example, some were giving away penny stocks as an incentive to use their apps. Now you can make a lot of money investing in penny stocks but you've got to take the approach that they do in private equity and venture, in which you need a lot of these stocks, because many of those things will just go to zero.

You have to think about what's the goal here: what are you giving me? Because you're probably not giving me anything great, you're giving me something meant to incentivize me to put money in the platform. Not incentivizing you to learn more about what you're doing, not incentivizing you to become a more sophisticated investor.

FinTech*: Do more gamification-related regulations seem likely, from what you've seen?*

Mathai-Davis: I think the regulators could overshoot this. Gamification is just too ubiquitous now. We're talking about basic extrinsic stimulation incentives to drive whatever engagement there is. I don't think Chairman Gensler is going to do anything that would in any way impact it negatively. But I do support cracking down on what I think is bad behavior (or at least not positive), which is the free giveaways types of things.

The thing is: There are other things you can borrow from game design that will drive experiences. We're not using gamification in the sense of, "we're going to give you this reward." We're more trying to create an intuitive experience for the user to make it easy for them to learn and understand what they're doing. I'm an ex-heavy video gamer. So I think: What could we borrow from gaming? Well, games have to be intuitive because, otherwise, you won't engage, and you'll leave. The games are also often free—it's engagement on the platform where the games make their money. So we're borrowing from game design to make the investing experience smooth and easy.

It's the Tesla experience. I was driving a sports car and a BMW before I got a Tesla last year. Now the BMW has got a million buttons. You're overwhelmed in these cars. Or it could even be a Toyota. You'll probably only use three or four buttons in any case. But I get into the Tesla, and there are just two knobs. The dashboard just tells you the basics: what direction am I driving, and where am I driving. That's what the investing experience should be. What am I doing, how are my holdings doing, what are the returns. Simple, easy and clean. You know what to do. That's proper gamification right there.

FinTech*: You've said that AI robo-investing and hedging will be the foundation for future investing apps and tools. What do you mean by this?*

Mathai-Davis: We use many deep learning algorithms that select securities, depending on what kits we're talking about. We do it as an ensemble: It's a democracy where the majority rule. It's a play on the wisdom of crowds. It's as if algorithms are an investment committee and each algorithm has its own vote. I see AI as the further advancement of predictable analytics. What you're doing is simply increas-

ing your probabilities that you're making the right securities selection. It's all probability analyses now—if I can improve my probabilities, theoretically I'm going to improve my outcomes. So, again theoretically, for the longer term, the introduction of predictive analytics should lead to better outcomes. Users or investors should more effectively determine the probability of any goals they're setting. I'm not saying this means outperforming the market. It's more about saying: this is what I'm trying to achieve, so how do I maximize probabilities to get to that point. AI permits that to happen—it's a more effective heuristic to do that.

Longer term, moving in that direction, you could argue that all you need is a portfolio manager and an analyst and a bunch of algorithms to do the rest of the work. But I don't believe in AI just running by itself because, at this point, it's still hard for the algorithms to understand the "garbage in, garbage out" syndrome. That happens quite a bit, especially with deep learning. You may get false positives in terms of correlations and other types of analytics. I see predictive analytics as something that's going to drive better outcomes—and that's something I care about.

If you can't in any way justify *why* you're putting data into an algorithm, you shouldn't put it in. If you can't make the qualitative argument that this is an important factor, don't put it in. Don't put in data just for the sake of it. Everything that we put in there—we provide a "here's why" rationale.

FinTech*: Are there other technological developments you're keeping an eye on?*

Mathai-Davis: The rise of NFTs, and how that's going to be a new rising asset class. I'm excited by that. Why aren't [entrepreneurs] looking at diversifying risk when funding movies, for example, democratizing access to capital for really cool ideas. Speaking as an entrepreneur, the biggest issue you typically have is getting access to capital, having a good distribution network. That's what gets me excited about NFTs. The commodification of products is really democratizing access to the marketplace.

Blockchain is going to be something very transformative. My view is that investing in crypto is going to be like venture investing was 20 years ago. It's high risk but if you look at it from an asset allocation perspective, if you didn't overweight into venture [back then], you regretted it. We have asset kits that are allocated into crypto. I'm a believer in it. I think crypto should be part of any properly diversified multi-asset strategy. So, for example, our global trends kit [offers] long short stocks, long short durations, commodities, FX and also gives you potential access to digital assets. The same thing goes for our emerging tech kit.

FinTech*: What does your near-term future look like?*

Mathai-Davis. We currently have four signature kits, five limited editions, and two select kits. We're planning on expanding that to 20 or 30 over the next couple of months. Bringing this to the individual investor changes the way they invest. You may have ideas you want to express but can't do it right now. You can't do it in a free trading app—that doesn't really

work. Or a traditional robo app where you have no personal connection with it at all. But now you can build a bunch of kits.

We have no fees at present. We're going to move to a subscription model. I call it the Netflix-ification of investing. Looking at the business over time, the fee structure to the asset-management business has caused tremendous damage to the quality of the investment product. It becomes this anchor that's correlated to the stock market. You're not going to take many risks in terms of products; you're going to be putting it in more traditional products. Over 80% of assets under management are controlled by four firms now. There is no substantial product differentiation. How many large-cap S&P 500 ETFs do you need? They're all pretty much the same thing now.

This is where we're going: We're throwing out the fee base. It's all about quality, telling the investor that you can do whatever you want. It's just got to be transparent to the average user. For our target, the mass affluent Gen Z/ Millennials, the parallel is their HBO Max, their Netflix accounts. Robinhood had a 2% fee base and no one signed up for it. Then they charged five bucks a month and everyone signed up [even though] it often translated to a much higher fee. But the customers understood it better—that was the difference. It was clear to them.

SEC ADVANCES BROAD THEORY OF REQUIRED DISCLOSURES OF SECURITY INCIDENTS

By Fran Faircloth and Nameir Abbas

Fran Faircloth (https://www.ropesgray.com/en/biographies/f/fran-faircloth) is an associate in Ropes & Gray's data, privacy & cybersecurity practice in Washington, D.C.

Nameir Abbas (https://www.ropesgray.com/en/biographies/a/Nameir-Abbas) is an associate in Ropes & Gray's data, privacy & cybersecurity practice in Washington, D.C.

Contact: Fran.Faircloth@ropesgray.com or Nameir.Abbas@ropesgray.com.

A recent SEC settlement has again demonstrated the Commission's continued attention to public companies' disclosures of cybersecurity incidents and its commitment to a broad notion of what constitutes such an incident. On August 16, the SEC entered a settlement agreement[1] with Pearson plc, a UK-based educational publishing company that is publicly traded on both the London Stock Exchange and New York Stock Exchange via ADRs. While Pearson made no admissions in the agreement, it will pay a $1 million civil penalty to settle the SEC's allegations that Pearson misled investors in its disclosures related to a 2018 cybersecurity breach.

Five key aspects of this settlement merit attention from a cybersecurity perspective be-

cause they are arguably more aggressive than the practices that have developed under state data breach laws:

- The breach appears to have involved primarily usernames and hashed passwords, but the SEC did not appear to treat hashed passwords differently than un-hashed passwords.
- The SEC focused on the presence of birth dates and email addresses in a significant percentage of the records, even though many state laws do not consider loss of such information to constitute a reportable data breach.
- The SEC suggested that a typical affirmation of cybersecurity as a value was misleading: "Protecting our customers' information is of critical importance to us. We have strict data protections in place and have reviewed this incident, found and fixed the vulnerability."
- The SEC likewise suggested a statement that is typically made when there is no direct evidence of misuse to be misleading: "While we have no evidence that this information has been misused, we have notified the affected customers as a precaution."
- The SEC's Order also considered the "breach at issue [to be] material" because the business of the company involved collecting large amounts of private data about children-without any reference to the direct financial impact of the breach on Pearson.

This enforcement action follows a series of statements and enforcement actions from the Commission stressing the importance of cybersecurity disclosures. Many public companies began including cybersecurity as a risk factor in their public disclosures after the SEC Division of Corporation Finance issued guidance[2] on such disclosures in October 2011. In February 2018 guidance,[3] the Commission again addressed the disclosure of cybersecurity risks and events. In that statement, the SEC stressed the importance of "accurate and timely disclosures of material events." Only two months later, in April 2018, the SEC settled charges with Yahoo![4] for failing to disclose a 2014 data breach until 2016. Between 2018 and 2021, there were no further settlement agreements related to disclosure of cybersecurity events, but earlier this summer, the SEC showed renewed interest in the area, settling charges against First American Financial Corporation[5] for alleged disclosure controls and procedures violations related to a cybersecurity vulnerability that potentially exposed customer information. The settlement with Pearson shows that such enforcement actions are likely to continue.

INCIDENT BACKGROUND AND IMPACTED DATA

On July 19, 2019, Pearson mailed a breach notification letter to customer accounts whose student and school personnel data had been impacted by a cybersecurity incident that began in November 2018. In that letter, Pearson said that affected data included student names, dates of birth, and email addresses, as well as administrator names, job titles, work emails, and

work addresses. On July 31, 2019, after being contacted by media, Pearson posted a public statement[6] to its website, which said that "exposed data was isolated to first name, last name, and in some instances may include date of birth and/or email address." The day after Pearson's online statement about the incident, its NYSE stock price declined by 3.3% (although the broader markets were down roughly 1% that day as well).

According to the settlement, the cyber-intrusion that Pearson experienced in 2018 involved the theft of "several million" rows of student and school personnel data, across approximately 13,000 customer accounts in the United States. The intrusion exploited an unpatched vulnerability on a server relating to a Pearson product called AIMSweb 1.0, used to track and enter student academic performance details (a new version of the product called AIMSweb Plus was not affected). The settlement alleges that Pearson received notice of a patch for the vulnerability in question months prior to the intrusion but failed to implement the patch until afterward.

In addition, the settlement alleges that school personnel usernames and hashed passwords for the product were also affected by the incident, which was not disclosed in the notification letter or in the statement on Pearson's website.

DISCLOSURES AND PUBLIC STATEMENTS

On its Form 6-K published on July 26, 2019, which covered the first six months of 2019, Pearson did not mention the incident, instead issuing only the same general, *hypothetical* risk statement that it had issued on prior Forms 6-K: "[r]isk of a data privacy incident or other failure to comply with data privacy regulations and standards and/or a weakness in information security, including a failure to prevent or detect a malicious attack on our systems, *could* result in a major data privacy or confidentiality breach causing damage to the customer experience and our reputational damage, a breach of regulations and financial loss" (emphasis added). Only five days later, on July 31, Pearson posted its online statement about the incident, prompting a drop in stock prices.

The SEC said that Pearson's general statement was insufficient to disclose that an actual breach had occurred. According to the settlement, Pearson failed to consider how that breach could have a material impact on its business that needed to be disclosed in its Form 6-K—especially given Pearson's recognition that it stored of "large volumes of personally identifiable information," including information about children. The settlement stated that a failure of Pearson's procedures led to the inadequate disclosures because the SEC considered the breach to be "material."

The SEC also took issue with alleged failures to

- Mention the loss of usernames and hashed passwords, in part because the hash at issue was an older and alleged unreliable hash algorithm. This is particularly noteworthy because many entities treat hashed data as equivalent to encrypted data (whose loss need not be disclosed),

and the state laws with that exemption have generally not specified a particular strength for encryption or hashing methods.

- Mention that birth dates and email addresses were taken even though they were taken for certain records.
- Temper the general statement: "Protecting our customers' information is of critical importance to us. We have strict data protections in place and have reviewed this incident, found and fixed the vulnerability."
- To note circumstantial evidence of misuse based on the identity of the attacker, even though there was no direct evidence of misuse.
- Consider the breach to be "material" given that the company's business involved collecting large amounts of private data about children.

TAKEAWAYS

Pearson is the third such settlement related to this issue from the Commission. In each of these settlements, as in its 2018 guidance, the SEC has stressed the importance of adequate disclosure controls and procedures, which are necessary to enable public companies to make timely disclosure of cybersecurity incidents.

The SEC appears to be pursuing an approach to data breach disclosures that is significantly more aggressive than is required under state data breach laws. Given the SEC's focus, it will be important for public companies to be particularly robust in their disclosures of data breaches and to avoid typical reassuring statements in their data breach disclosures unless those are fully supported in the circumstances.

In the Pearson settlement, the SEC noted that "Pearson's processes and procedures around the drafting of its July 26, 2019 Form 6-K Risk Factor disclosures and its July 31, 2019 media statement failed to inform relevant personnel of certain information about the circumstances surrounding the breach." The Pearson settlement is a reminder that controls and procedures are necessary to ensure that the individuals who are in charge of issuing disclosures have the necessary information to meet their obligations. Public companies would be wise to assess how incidents are reported to key personnel involved in disclosure-related decisions and evaluate whether additional controls or procedures could help to provide appropriate and timely reporting.

ENDNOTES:

[1] https://www.sec.gov/litigation/admin/2021/33-10963.pdf.

[2] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[3] https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[4] https://www.sec.gov/news/press-release/2018-71.

[5] https://www.sec.gov/news/press-release/2021-102.

[6] https://www.pearson.com/news-and-research/announcements/2019/07/pearson-customer-notification.html.

SEC SPAT WITH COINBASE PREVIEWS COMPLEX LEGAL BATTLE OVER CRYPTO

By Todd Ehret

Todd Ehret is a senior regulatory intelligence expert at Thomson Reuters Regulatory Intelligence.

A recent public exchange between U.S. Securities and Exchange Commission Chair Gary Gensler and top executives of Coinbase, the largest U.S. cryptocurrency exchange, offers a preview of what will likely be a lengthy and complex battle over the legal and regulatory framework surrounding cryptos.

The former chairman of the U.S. Commodity Futures Trading Commission ("CFTC"), Christopher Giancarlo also weighed in, without directly criticizing or taking sides in the debate, saying it is a challenge to apply "90-year-old statutes" against new innovation that was never contemplated.

In testimony before the U.S. Senate Banking Committee in mid-September, Gensler warned that cryptocurrency exchanges such as Coinbase should register with the regulator. In response to a hypothetical question from Senator Elizabeth Warren mentioning Coinbase, Gensler said, "they haven't yet registered with us, even though they have dozens of tokens that may be securities."

His comment is the latest jab in a series of back-and-forth punches between the SEC and top executives at Coinbase over regulatory uncertainty surrounding the cryptocurrency industry. The comment came just days after a lengthy Twitter thread by Coinbase CEO Brian Armstrong and a blog post by Coinbase Chief Legal Officer Paul Grewal, which criticized the agency's handling of the firm's plans to roll out a lending product the SEC has determined to be a security.

The dispute between the SEC and Coinbase is indicative of the complex and uncertain regulatory and legal environment surrounding cryptos.

GENSLER'S BEEF WITH COINBASE AND POTENTIAL REGULATORY LAND GRAB

At the heart of the legal dispute between the SEC and Coinbase is regulatory jurisdiction related to the rapidly growing and evolving crypto marketplace. More specifically, the definition of whether cryptocurrencies and related stablecoins are legally defined as securities and are therefore subject to regulation by the SEC.

Gensler has asserted, without offering specifics, that some digital assets and platforms are operating as, or offering, securities, which would bring them under the SEC's oversight. He also has asked Congress for more specific authority in areas that may be unclear or outside the SEC's jurisdiction.

In the case of Coinbase, the SEC has taken issue with the firm's planned rollout of its "Coinbase Lend" platform. Grewal wrote in a public blog[1] that the SEC has issued Coinbase with a so-called "Wells Notice" that it intends to legally charge the company if it proceeds

with plans to launch the product, which allows users to earn interest by lending digital assets. Coinbase disputes that the Lend program is a security. Grewal wrote that the program is based on the USD Coin, or USDC, a cryptocurrency linked to the U.S. dollar. Such cryptocurrencies linked to an underlying asset are called "stablecoins."

"Customers won't be 'investing' in the program, but rather lending the USDC they hold on Coinbase's platform in connection with their existing relationship. And although Lend customers will earn interest from their participation in the program, we have an obligation to pay this interest regardless of Coinbase's broader business activities. What's more, participating customers' principal is secure and we're obligated to repay their USDC on request," Grewal said.

A perceived lack of communication or cooperation by the regulator is what appears to be causing Coinbase to speak out publicly.

Despite the SEC's repeated encouragement for the cryptocurrency industry to "come in and talk to us," Grewal and Armstrong said Coinbase has been trying to engage with the agency for nearly six months without much response. "The SEC told us they consider Lend to involve a security, but wouldn't say why or how they'd reached that conclusion," Grewal wrote.

"A healthy regulatory relationship should never leave the industry in that kind of bind without explanation. Dialogue is at the heart of good regulation," he said.

Armstrong said on Twitter: "If we end up in court we may finally get the regulatory clarity the SEC refuses to provide. But regulation by litigation should be the last resort for the SEC, not the first."[2] The SEC declined to comment on the exchange. "The SEC does not comment on the existence or nonexistence of a possible investigation," a representative said.

Gensler is seeking more authority for the agency to oversee a world he has described as a "Wild West" riddled with fraud and investor risk. In his Senate testimony recently, he asked for more resources to meet the growing regulatory projects.

The fact that Coinbase has gone public with the dispute with the regulator suggests a public relations effort to rally support from the crypto and legal communities. Several days later, Coinbase announced in a blog post it would not launch the program. "As we continue our work to seek regulatory clarity for the crypto industry as a whole, we've made the difficult decision not to launch the USDC APY [Annual Percentage Yield] program," Coinbase stated on its blog post.

GIANCARLO WEIGHS IN

In an interview on September 9, 2021 on CoindeskTV, former CFTC Chairman Christopher Giancarlo shared his thoughts on a wide range of crypto-related issues from central bank digital currencies to the complex legal and regulatory issues surrounding cryptos.

Giancarlo is now a senior attorney with Willkie Farr & Gallagher LLP, and advocates for the blockchain and cryptocurrency industries. Giancarlo said that during his time

at the CFTC, they found that existing rules "weren't applicable to this new innovation, to crypto itself."

"It is important for this new innovation that we not apply 90-year-old statutes, which is effectively what we have for the Commodities Exchange Act and the Securities Exchange Act, against a new innovation that was never contemplated in the 1930s when those statutes were written."

Without directly commenting on the Coinbase and SEC uncertainty, Giancarlo said that when he was at the CFTC the "priority was to clarify rules and then look at enforcement actions." To do otherwise would put firms in unwitting legal jeopardy.

When discussing the issue of jurisdiction, Giancarlo said, "ultimately, it will be the courts that will have to determine jurisdiction and apply the security laws to these asset classes, and I'm optimistic that Congress steps in. Congress in the last few months has really recognized crypto . . . and has woken up to this technology and its power and potential."

Cryptos and blockchain are a chance to modernize finance and solve the worst elements of its existing structure: "its slowness, its expensiveness and, most unfortunate, its exclusiveness," he said. "We need to see it as revolutionary and be willing to be flexible with our existing models and look to this innovation to modernize shortcomings."

ENDNOTES:

[1] https://blog.coinbase.com/the-sec-has-told-us-it-wants-to-sue-us-over-lend-we-have-no-idea-why-a3a1b6507009.

[2] https://twitter.com/brian_armstrong/status/1435439291715358721 (thread).

FORMER FINRA ENFORCEMENT CHIEF SAYS Reg BI BRINGS NEW COMPLIANCE LIABILITY

By Richard Satran

Richard Satran is an editor at Thomson Reuters Regulatory Intelligence.

Regulation Best Interest ("Reg BI") has brought new challenges for compliance, even though it looks a lot like the previous suitability rule, former Financial Industry Regulatory Authority enforcement chief Susan Schroeder said in a recent interview. When combined with enhanced surveillance tools coming on line, "the door is wide open for data-driven approaches" in a wider range of suitability cases involving firms' products and sales practices.

Schroeder now looks at the potential impact of Reg BI from the private side as vice chair, Securities & Financial Services Department, of the law firm Wilmer Cutler Pickering Hale and Dorr LLP, after nearly a decade in FINRA enforcement and management. She held key positions at FINRA as the industry self-regulator worked with the Securities and Exchange Commission in adopting Reg BI, which marked the first major change in brokerage industry sales practice rules in decades.

Schroeder, who left FINRA in 2019, said in this interview that while Reg BI did not bring a dramatic change for brokers since it "borrowed

pretty liberally from the FINRA suitability rule," for compliance, there will be bigger challenges since it has "the potential for much more compliance liability."

In the interview, she said she saw enforcement actions on the horizon that will require firms to show how they have mitigated conflicts of interest in areas such as volatility products, excessive trading and even actions in which supervisory failures alone create violations—absent of other transgressions. The rule changes also raise potential for the SEC to take actions once handled largely by FINRA.

FinTech: Going forward, do you see compliance liability rising under Reg BI as judgment calls and interpretations are required? For example, the mitigation versus elimination of conflicts of interest? Is it all about documentation? Or is it a lot more than that?

Schroeder: Reg BI creates the potential for much more compliance liability because of the duty of compliance. Under Reg BI, it's a violation to have faulty supervisory policies and procedures—even if there are no problematic customer trades or disclosures. If regulators look to hold individuals accountable (and they always do), the compliance professionals responsible for creating the firm's supervisory structure could find themselves the subject of a lot of scrutiny.

FinTech: The elimination of the control factor in determining excessive trading will make it easier to pursue actions. When you combine this with account level surveillance with CAT do you see this as a game changer?

Schroeder: Now that the SEC and FINRA no longer need to show that a broker "controlled" the customer's account in order to prove that the broker excessively traded in that account, I think the door is wide open for data-driven approaches. The SEC experimented with that approach a few years ago in a case against two individual brokers, Dean and Fowler, where the SEC alleged that the brokers controlled the accounts—but it also alleged that they recommended a quantitatively unsuitable strategy, and it relied on statistics in support of its claim. At the trial, the SEC did not even elicit testimony from all the victims. It relied on numbers. And it won.

FinTech: Do you see a Reg BI type concern from the recent spate of volatility product actions and the recent SEC action against S&P over alleged flaws in its product? Have firms done enough to review products for Reg BI vulnerabilities?

Schroeder: Regulators are likely to use Reg BI as a powerful tool when investors are affected by performance issues in complex products. Brokers have to exercise due diligence to form a reasonable basis to believe that a security is suitable for at least some investors. Under Reg BI, regulators can use that due diligence obligation as the basis to charge firms with failures when they sell complex products that don't perform. Even if the features of a product are not unsuitable for a customer, the regulators can still take the position that the broker didn't understand the product and therefore it violated Reg BI when it sold it. Firms selling complex products should document

their initial due diligence process and make sure they refresh their diligence frequently.

FinTech: You've said in a WilmerHale.com client advisory that Reg BI in a sense is "not new" since it is built on the existing suitability standard. FINRA's action to update regulations to conform with Reg BI amounted to tweaks. So do you mean that its form or shape is the same even if there is a new standard of care with a fiduciary-style rule?

Schroeder: When the SEC adopted Reg BI, it borrowed pretty liberally from the FINRA suitability rule and acknowledged it was doing so. The three pillars of Reg BI's "duty of care" correlate with the three types of suitability that FINRA identified in its rule. So I think enforcement actions based on violations of the "duty of care" are likely to look an awful lot like FINRA suitability actions-except they'll be brought by the SEC and FINRA.

FinTech: From a compliance point of view how is Reg BI different from suitability?

Schroeder: Reg BI is more than just the duty of care, which echoes the suitability rule. There are aspects of Reg BI that are new for broker-dealers, such as the duty to identify and mitigate or eliminate conflicts of interest. And Reg BI is also one of a handful of SEC rules that imposes an affirmative obligation to establish, maintain and enforce policies and procedures to achieve compliance with the regulations. That means that inadequate supervisory policies or procedures are enough for an enforcement action—no underlying suitability violation required.

FinTech: FINRA said that in the first six months of Reg BI exams firms were largely compliant. Do you think FINRA was just being nice? Or will Reg BI begin to have a larger impact going forward?

Schroeder: During the first six months after Reg BI's implementation date, the SEC and FINRA were looking for "good faith efforts" to comply, and they generally found firms were, in fact, trying in good faith to comply. But the SEC has since made it clear that the "good faith" days are over. I think we can expect significant Reg BI cases coming out of the SEC. We can expect "conflicts interest cases" similar to SEC cases that we would see against investment advisers in the past, and we can expect suitability cases where the SEC uses the legal frameworks FINRA has used in the past.

EXPLORING A DIGITAL EURO

By Jens Weidmann

Dr. Jens Weidmann is the President of Deutsche Bundesbank. The following is excerpted from remarks that he gave at a digital symposium held by the Bundesbank and the People's Bank of China on September 14, 2021.

The main theme of our conference is "Fintech and the Global Payments Landscape—exploring new horizons." Unfortunately, the pandemic forces us to hold it as a digital event. If we had been able to meet here in person, I would have recommended a visit to the Bundesbank's Money Museum and the current numismatic special exhibition on the topic of "Money Creators. Who decides what's

money?" In the dawning age of digital currencies, that is a highly relevant question indeed. Crypto tokens and other innovations in finance are challenging established views on what constitutes money.

The exhibition takes a historical perspective and thereby teaches us important lessons about creating money in the future. For example that our success as a money creator depends on the trust of those who are supposed to use that money. That it is not necessarily the state that creates money but that creating money means having power. And that the form and use of money has always been changing.

Paper money, for instance, was first introduced in China about a thousand years ago. This innovation eventually transformed the payments system. Today, digitalization is on the cusp of overhauling payments.

Central banks have to work out how to respond to this challenge.[1] One possibility is the issuing of central bank digital currencies ("CBDCs"). According to a survey by the Bank for International Settlements ("BIS"), the share of central banks conducting work on CBDCs for general or wholesale use rose to 86% last year.[2] Many of them have made significant progress.

In the public debate, CBDCs that can be used by consumers and businesses have taken center stage. And it is on such retail CBDCs that I would like to focus in my talk. The People's Bank of China has been playing a pioneering role in the development of such a digital currency and we are looking forward to gaining fresh insights into its projects.

A DIGITAL EURO

[In July], the Eurosystem launched a project to investigate key questions regarding the design of a CBDC for the euro area.[3] The aim of the investigation is to prepare us for the potential launch of a digital euro. Experiments have already shown that, in principle, a digital euro is feasible using existing technologies.

However, introducing a CBDC is not an end in itself. There are various conceivable reasons why a central bank might introduce a digital currency. And its intended purpose will have important implications for its design: it is a matter of "form follows function." Accordingly, future CBDCs may differ in form and functionality across currency areas. Of course, CBDCs should only be issued if the perceived benefits outweigh any potential drawbacks or risks. Thus, a digital euro needs to provide a clear value added to euro area citizens.

To start with, a CBDC is often expected to lower transaction costs and to raise efficiency in payments, financial markets and the real economy.[4] It could also stimulate innovative services and give rise to new business models. Moreover, a key factor in my view is that a digital euro would enable consumers and businesses to pay with central bank money in a digital environment. This is a unique feature that the private sector cannot replicate. As my ECB colleague Fabio Panetta has stressed, a digital euro would have "no liquidity risk, no credit risk, no market risk,"[5] in this way resembling cash.

Thus, private households and firms would be

given an additional way of using public money, just as the use of cash is waning. Indeed, according to a representative Bundesbank survey, the share of cash payments in point of sale transactions made by German consumers dropped from 74% in 2017 to 60% last year.[6] Admittedly, the pandemic may have had an impact on payment behavior that could fade again. But the underlying trend is clear. And some experts recommend preparing for a future in which cash may no longer be king.

Beyond safety, another feature of cash that many people value highly is its anonymity. You don't need to identify yourself when you pay cash. It is therefore not surprising that in a public consultation of the Eurosystem both consumers and professionals considered privacy the most important feature of a digital euro.[7]

The protection of privacy would thus be a key priority in terms of maintaining people's trust. European data protection rules would have to be complied with. Nevertheless, a digital euro would not be as anonymous as cash. In order to prevent illicit activities such as money laundering or terrorist financing, legitimate authorities would have to be able to trace transactions in individual, justified cases.

Overall, the declining use of cash is a major reason for many central banks to consider offering CBDCs. But let there be no mistake about this: the Eurosystem will continue to provide access to banknotes as long as people want cash. A digital euro would be meant to complement cash, not to replace it. The goal would be to broaden the choice of payment means available to consumers in a world that is becoming more and more digital.

You may be familiar with a piece of proverbial advice: check that the ladder is leaning against the right wall before climbing it. That's a warning that should be heeded when it comes to CBDCs, too. We need to think carefully about what the purpose would be in issuing digital central bank money. And we have to mind and curb the risks that its introduction may imply.

For example, since a CBDC is a substitute for bank deposits, at least to some extent, it might bear important risks for the functioning of the financial system and the implementation of monetary policy. If, in times of crisis, consumers were to rush to exchange their sight deposits for CBDCs on a massive scale, financial stability could be jeopardized.

Depositors could also shift their funds into CBDCs only gradually and over a long period. In this scenario, banks would still lose a convenient source of stable funding. To make up for it, they may increasingly turn to other sources like the bond market or to the central bank to finance their activities. This may affect the amount of credit which commercial banks supply to the economy. The impact on the equilibrium depends on various factors and is not clear-cut to predict.[8]

Still, the established roles in the financial system could be transformed. And this could apply to more than just commercial banks. The central bank might end up directly interacting with consumers, attracting deposits on a grand scale and extending its balance sheet substantially. Hyun Song Shin from the BIS has pointed out that the central bank could

leave "a much larger footprint" on the financial system because of this.[9]

We have a two-tiered monetary and banking system with a clear division of tasks between the central bank and commercial banks. According to Princeton economist Markus Brunnermeier, it is "probably the most pronounced public-private partnership we have in our economies."[10] It should not be gambled with.

However, this does not call for banks to be protected like an endangered species, either. On the upside, CBDCs could spur on competition among banks and promote new services. Some banks might also become more cautious and reduce the potential for banking stress. But designing a CBDC involves curbing its risks. In order to prevent excessive withdrawals of bank deposits, it has been suggested that a cap be placed on the amount of digital euro that each individual can hold. Or that digital euro holdings in excess of a certain limit could be rendered unattractive by applying a penalty interest rate.[11]

Proposals like these highlight the difficult trade-offs central banks face. CBDCs should be designed in a way that allows its users to reap its potential benefits as fully as possible, while keeping its risks and potential side effects at bay. It should be sufficiently attractive for users to accept it. At the same time, CBDCs should not be too attractive since, otherwise, they might disrupt the financial system.

The design of a potential digital euro is still vague. It may not be a jack-of-all-trades. To my mind, a gradual approach might make sense given the risks involved—that means a digital euro with a specific set of features and the option to add further functionalities later.

CROSS-BORDER INTEROPERABILITY OF CBDCS

One feature lending appeal to CBDCs would be their use for cross-border payments. At the moment, such transactions are still relatively inefficient and expensive. In a joint report, a group of international institutions recently emphasized that "faster, cheaper, more transparent and more inclusive cross-border payment services would deliver widespread benefits to citizens and economies worldwide."[12]

However, if a digital euro were accessible for non-residents, this could impact on capital flows and euro exchange rates. In the event of high foreign demand, a digital euro would substantially extend the balance sheet of the Eurosystem. Broad-based international use could also drive a "euroization" of financial systems in other currency areas. And, by the same token, the issuance of CBDCs by foreign countries could have converse effects on the euro area.

What this calls for is international and multilateral collaboration. Or, put simply, finding some common ground. In my view, it is crucial that CBDCs function together, not against each other. Enabling cross-border payments through interoperability should be an important element of all the ongoing discussions on CBDCs.

At the G20 level, discussions have already started. And the report that I mentioned earlier

suggests different degrees of possible cooperation, ranging from basic compatibility with common standards to the establishment of international payment infrastructures.

I think that enhancing cross-border payments should also be an important topic at the G7 level under the German presidency next year. We should take that opportunity to delve deeper into the international aspects of CBDCs. Connected with each other, CBDCs could make a real difference to the efficiency of cross-border payments.

REGULATING BIGTECH

Game-changing qualities of money are nothing new. More than 2,600 years ago, in what is today Turkey, the kingdom of Lydia minted the first coins the world had ever seen. According to the American anthropologist Jack Weatherford, the invention of coins fostered a "variety and abundance of commercial goods that quickly led to another innovation: the retail market."[13] Neighboring Greece not only adopted these innovations, but centered its public life on the marketplace—the agora.[14] In Weatherford's view, "Greece (. . .) arose from the marketplace and commerce. Greece had created a whole new kind of civilization."[15]

To what extent the digitalization of money will be a game-changer, remains to be seen. Digitalization can improve transparency, as consumers are able to gain an overview of the market with just a few clicks. But it could also serve to concentrate power and cripple competition.

In recent years, private stablecoin initiatives have intensified concerns about the increasing role of bigtech firms in payments and their growing market power in general. The large digital platforms feature strong network effects and economies of scale that can facilitate market concentration. Once a provider becomes dominant in its market, it could hamper competition, dictate higher prices and push up profit margins at the expense of consumers.

What distinguishes the digital platforms of today from networks created in the past is the special role played by data. Large volumes of data—"big data"—allow platforms to identify patterns, create profiles and predict behavior. For instance, an academic study found that, once you have given 300 "likes," Facebook may know you better than your friends and family do.[16]

Customer data can help to improve the services of platforms or to better target advertising. But they are also a treasure trove that can help platform providers to eke out a competitive edge in other markets. Moreover, by creating entire ecosystems, bigtech firms could enhance network effects and customer experience, thereby stimulating user activities, which generate yet more data.

Thus, self-reinforcing loops and "lock-in" effects may tie users to one platform and exclude competitors.[17] Some observers have been reminded of "Hotel California," the famous song by the American rock band The Eagles: it's such a lovely place, with plenty of room; but once inside you can never leave.

If competition is hampered by the rising market power of bigtech firms, this needs to be ad-

dressed by competition law and policy in a reliable way. Concerns regarding data protection fall beyond the scope of central banks, too.

However, some important issues in digital finance are part of banking supervision. In this respect, it's a matter for central banks and financial regulators, too. The more so as here market dominance can quickly turn into systemic relevance. Just think of a platform that provides crucial services to a large number of banks.

In the case of bigtech, the traditional demarcations that separate the roles of regulating institutions involved may become blurred.[18] The different actors should therefore collaborate more intensively—both within jurisdictions and, with respect to global platforms, also across borders.

I would consider the establishment of broad supervisory colleges an appropriate approach. Such "cross-disciplinary, cross-geographic colleges" could enhance information exchange and cooperation. Overall, the state has to set robust ground rules for competition and make sure that everybody plays by those rules. At the end of the day, both governments and markets should serve people—not the other way around. I am also convinced that regulatory policy should help people use their personal data as they see fit and ultimately strengthen consumer sovereignty.

Here, too, a digital euro could be instrumental. The Eurosystem has no commercial interest in user data or behavior. A digital euro could therefore help to safeguard what has always been the essence of money: trust.

BEYOND CBDC

Distributed ledger technology ("DLT") is often seen as harboring great potential, for instance when it comes to enabling programmable payments. Indeed, a programmable payment medium would be practical for applications like smart contracts, machine-to-machine payments, internet-of-things-payments or pay-per-use payments.[19] But this is not necessarily a case for CBDCs. An alternative solution might be for the private sector to tokenize commercial bank money. The EU's proposed "MiCa" regulation establishes a framework for payment tokens that the private sector can work within to develop payment solutions needed in a digitalized economy.

Still, recipients of large payments may prefer settlement in central bank money since it harbors no risk of default. If we were able to build a bridge between private blockchain networks and the existing payment infrastructure, DLT-based trade could be settled in central bank money without requiring CBDCs. This is why Bundesbank experts are investigating a "trigger solution," which could allow smart contracts to trigger conventional TARGET2 transactions.[20]

Another possibility would be for central banks themselves to issue a token to be used by commercial banks. Such a wholesale CBDC could, for example, complement innovative ways of exchanging and settling financial assets. Given that the tokenization of assets is

becoming increasingly prominent in the world of finance, such a central bank token could provide an important benefit.

In any case, the Eurosystem will further investigate the potential of innovations beyond CBDCs and continue to improve its existing payments infrastructures. At the same time, we should make sure that our activities in the field of digital currency do not discourage the private sector from developing convenient and efficient applications for consumers and businesses.

In a market economy, offering innovative payment solutions to the public and interacting with customers is primarily a task for the private sector. Central banks' task is to provide critical infrastructures as a basis for others to develop and supply their services, thereby acting as a catalyst.

CONCLUSION

In the 13th century, the Venetian merchant Marco Polo travelled to Asia and later gave a vivid account of the wonders he had seen. In particular, he described how something resembling sheets of paper was made from the bark of mulberry trees and was universally accepted as money throughout China. Polo's reports were met with sheer disbelief in Europe. It was only centuries later that paper money became common in Europe, too. The innovations we are talking about today will spread much faster.

Central banks need to be at the cutting edge of technology. Otherwise, they cannot provide the backbone of payment systems and offer safe and trusted money for the digital age. This has prompted all major central banks to start exploring issuance of CBDCs. However, our success as a money creator will depend not so much on speed, but on the trust of those who are supposed to use the money.

ENDNOTES:

[1]Deutsche Bundesbank, Digital money: options for payments, Monthly Report, April 2021, pp. 57-75.

[2]Bank for International Settlements (2021), Ready, steady, go?-Results of the third BIS survey on central bank digital currency, BIS Papers, No 114.

[3]European Central Bank, Eurosystem launches digital euro project, press release, July 14, 2021.

[4]Bordo, M. and A. Levin (2017), Central Bank Digital Currency And The Future Of Monetary Policy, National Bureau of Economic Research, Working Paper, No 23711; Keister, T. and D. Sanches (2019), Should Central Banks issue Digital Currency?, Federal Reserve Bank of Philadelphia, Working Paper, No 19-26.

[5]Panetta, F., Preparing for the euro's digital future, blog post, July 14, 2021.

[6]Deutsche Bundesbank, Payment behaviour in Germany in 2020, 14 January 2021.

[7]European Central Bank (2021), Eurosystem report on the public consultation on a digital euro.

[8]Chiu, J., M. Davoodalhosseini, J. Jiang and Y. Zhu (2020), Bank market power and central bank digital currency: Theory and quantitative assessment, Bank of Canada, Staff Working Paper, No 2010-20; Andolfatto, D. (2018), Assessing the impact of central bank digital currency on private banks, Federal Reserve Bank of St. Louis, Working Paper, No 2018-25.

[9]Shin, H. S., Central banks and the new

world of payments, speech given on June 30, 2020.

[10]Brunnermeier, M., keynote speech at the Academic Colloquium in Honour of Otmar Issing, June 29, 2021.

[11]Bindseil, U., Tiered CBDC and the financial system, European Central Bank, Working Paper, No 2351, January 2020; Panetta, F., interview with Der Spiegel, February 9, 2021.

[12]Bank for International Settlements, Central bank digital currencies for cross-border payments, Report to the G20, July 2021.

[13]Weatherford, J. (1997), The History of Money, Three Rivers Press, New York, p. 31.

[14]Weidmann, J., Exploring the agora: Lessons for a more stable economic and monetary union, speech given on August 30, 2018.

[15]Weatherford, J. (1997), op. cit., p. 37.

[16]Youyou, W., M. Kosinski and D. Stillwell (2015), Computer-based personality judgments are more accurate than those made by humans, Proceedings of the National Academy of Sciences of the United States of America, Vol. 112, pp. 1036-1040.

[17]Bank for International Settlements, CBDCs: an opportunity for the monetary system, BIS Annual Economic Report 2021, pp. 65-95.

[18]Carstens, A., S. Claessens, F. Restoy and H. S. Shin (2021), Regulating big techs in finance, BIS Bulletin, No 45.

[19]Deutsche Bundesbank, Money in programmable applications, Monthly Report, April 2021, p. 62; Deutsche Bundesbank, Money in programmable applications-Cross-sector perspectives from the German economy, December 21, 2020.

[20]Deutsche Bundesbank, The Bundesbank's trigger solution, Monthly Report, April 2021, p. 67.

FINTECH LAW REPORT: AUGUST/SEPTEMBER 2021 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

Federal Banking Agencies Publish FinTech Diligence Guide for Community Banks

On August 27, 2021, the Office of the Comptroller of the Currency (the "OCC"), the Board of Governors of the Federal Reserve System (the "Board"), and the Federal Deposit Insurance Corporation (the "FDIC" and, together with the OCC and the Board, the "Federal Banking Agencies") published a user-friendly, concise due diligence guide for community banks considering relationships with financial technology companies (the "Community Bank Fintech Guide").[1] The Community Bank FinTech Guide "provides information relating to six common areas of due diligence discussed in existing supervisory guidance,"[2] with respect to a fintech company's ability to meet the bank's needs, including:

- an evaluation of the fintech company's business experience, strategic goals, and

overall qualifications in conducting the applicable activity;

- an evaluation of the fintech company's financial condition and prospects for long-term viability;
- an evaluation of the fintech company's sophistication with respect to the applicable legal and regulatory framework;
- an evaluation of the fintech company's risk management policies and controls, risk appetite, and the experience and independence of its risk managers;
- an evaluation of the fintech company's information security policies and processes for handling the types of information and data that may or will be exposed through the proposed relationship, and
- an evaluation of the fintech company's operational resilience, including its business continuity and disaster recovery plans, backup systems and service downtime expectations.[3]

Each category of due diligence elaborates on the relevant considerations, potential sources of information, and illustrative examples.[4] The Community Bank FinTech Guide emphasizes that the "scope and depth of due diligence performed by a community bank will depend on the risk to the bank from the nature and criticality of the prospective activity."

You can access the Community Bank FinTech Guide here: https://www.occ.gov/news-issuances/news-releases/2021/nr-ia-2021-85a.pdf

Federal Reserve Publishes Paper on FinTech-Community Bank Partnerships

On September 9, 2021, the Board published a paper entitled "Community Bank Access to Innovation through Partnerships" (the "FinTech Partnership Paper")[5] that describes "the landscape of partnerships between community banks and fintech companies" using "insights gathered from extensive outreach with community banks, fintechs, and other stakeholders."[6] The FinTech Partnership Paper was published as one part of the Board's larger initiative to promote access to innovation for community banks that also includes the Community Bank FinTech Guide and the proposed interagency guidance on managing risks associated with third-party relationships.[7] The FinTech Partnership Paper is "intended to serve as a resource for community banks as they embark on responsible innovation" and to provide "an overview of the evolving landscape of community bank partnerships with fintechs, including the benefits and risks of different partnership types, and key considerations for engaging in such partnerships."[8]

The FinTech Partnership Paper addresses (i) "partnership types and their associated benefits, risks, and challenges" and (ii) elements that contribute to successful partnerships as identified by industry participants.[9] Partnership types identified include operational technology partnerships, customer-oriented partnerships, and front-end fintech partnerships (also known as banking-as-a-service partnerships).[10] The FinTech Partnership Paper does not provide specific industry examples of the partnership

types, but does provide the following general descriptions:

> ● *Operational technology partnerships, wherein a community bank deploys third-party technology to its own processes or infrastructure to improve efficiency and effectiveness.*
>
> ● *Customer-oriented partnerships, wherein a community bank engages a third-party to enhance various customer-facing aspects of its business, and the bank continues to interact directly with its customers.*
>
> ● *Front-end fintech partnerships, wherein a bank's infrastructure is combined with technology developed by a fintech, with the fintech interacting directly with the end-customer in the delivery of banking products and services.*[11]

Elements of successful fintech-bank partnerships identified in the FinTech Partnership Paper include:

- a holistic bank approach and commitment to innovation that aligns the bank's long-term strategy, leadership, and resources to address customer demands and gain efficiencies;
- an alignment of priorities and objectives between the fintech partners and the bank evidenced by alignment on customer service and second-look regulatory safeguards and redundancies, and
- a thoughtful and tailored approach to technical infrastructure connectivity that considers the bank's current capabilities and speed of adoption (*i.e.*, text file interfaces versus API interfaces), whether the partnership will be customer facing, and what types of data will be shared between the parties.[12]

You can access the FinTech Partnership Paper here: https://www.federalreserve.gov/publications/community-bank-access-to-innovation-through-partnerships.htm

You can access a transcript of the Remarks here: https://www.federalreserve.gov/newsevents/speech/bowman20210909a.htm

FTC Staff Asks Federal Reserve Board to End Routing-Based Incentives in Regulation II Revisions

On August 11, 2021, the staffs of the Federal Trade Commission's Bureau of Competition, Bureau of Economics, and Bureau of Consumer Protection (collectively, the "FTC Staff") submitted a comment letter (the "FTC Comment Letter")[13] to the Board in response to the Board's notice of proposed rulemaking ("NPR")[14] and invitation to comment on "proposed changes to Regulation II (Debit Card Interchange Fees and Routing) ("Regulation II") to clarify that debit card issuers should enable, and allow merchants to choose from, at least two unaffiliated networks for card-not-present debit card transactions, such as online purchases."[15] In the FTC Comment Letter, the FTC Staff "applauds the Board's proposed clarification, which addresses some issuers' failure to fully recognize that card-not-present ("CNP") transactions are a 'type of transaction' under the existing Regulation II" and suggests

that the Board make additional revisions that the FTC Staff believes will strengthen Regulation II.[16] Specifically, the FTC Staff calls on the Board to adopt revisions that would (i) ensure that debit card networks are not incentivized to evade Regulation II's two network mandate and (ii) "prohibit debit card networks from paying incentives to an issuer based on how electronic debit transactions are routed by merchants using that issuer's debit cards."[17]

The FTC Staff alleges that "routing based incentives" included in the agreements between the debit card networks and the card issuers are intended to encourage the issuers to disable certain features—including, notably, CNP transaction capabilities—for the alternative network which serves to "eviscerate merchant routing choice."[18] Accordingly, the FTC Staff recommends that "the Board revise 12 C.F.R. § 235.7(a)(3) or its associated commentary to expressly prohibit payment card networks from using routing-based incentives."[19]

Additionally, the FTC Staff urges the Board to consider other types of functionality beyond CNP functionality that might enable issuers and card networks to limit merchant routing choice. In its letter, the FTC Staff recalls that the Board did not previously address routing-based incentives because it assumed that issuers would have "limited ability to control how transactions would be routed."[20] The FTC Staff argues that, in addition to CNP transactions, card networks and issuers have the ability to effectively control routing by enabling or disabling current and future features, including dual message capability and PIN authenticated transactions.[21]

You can access the NPR, which was published in the Federal Register on May 13, 2021, here: https://www.federalregister.gov/documents/2021/05/13/2021-10013/debit-card-interchange-fees-and-routing.

You can access the full text of the FTC Comment Letter here: https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-board-governors-federal-reserve-system-docket-no-r-1748-rin-7100-ag15-debit-card/fed_board_staff_comment_p859910.pdf.

FFIEC Issues New Guidance on Authentication and Access to Digital Financial Institution Services

On August 11, 2021, the Federal Financial Institutions Examination Council ("FFIEC"), on behalf of its members,[22] issued new guidance on "Authentication and Access to Financial Institution Services and Systems" (the "FFIEC Guidance").[23] The FFIEC Guidance replaces the FFIEC-issued *Authentication in an Internet Banking Environment* (2005) and the *Supplement to Authentication in an Internet Banking Environment* (2011), which addressed internet-based products and services.[24] The FFIEC Guidance, like the guidance it replaces, applies to consumer and business customers but also extends to other "users accessing financial institution information systems" including employees, board members, third parties and other systems (such as applications and devices).[25] The expanded coverage of the FFIEC Guidance reflects the FFIEC's recognition that effective risk management of cybersecurity threats requires that financial institutions address "business and consumer customers, employees, and third parties that access digital

banking services and financial institution information systems."[26]

The FFIEC Guidance articulates that single-factor authentication as the only control mechanism is inadequate, and that "single-factor authentication with layered security has shown to be inadequate for customers engaged in high-risk transactions and for high-risk users."[27] Instead, the FFIEC Guidance provides that "[w]hen a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, [multi-factor authentication] or controls of equivalent strength as part of layered security can more effectively mitigate risks."[28] The FFIEC Guidance does not define "high-risk transactions" or "high-risk users," but does note certain influencing characteristics. For high-risk transactions, these include the dollar amount and volume, the sensitivity and amount of information accessed, the irrevocability of the transactions and the likelihood and impacts of fraud.[29] Identified characteristics of high-risk users include those with access to critical systems or data and those with higher privileged or remote access to systems.[30]

The FFIEC Guidance specifically addresses access to financial institutions' systems by data aggregators and other customer-permissioned entities ("CPEs"), noting that "[a] comprehensive risk management program includes an assessment of risks and effective mitigating controls . . . when CPEs access a financial institution's information systems and customer information."[31]

Consistent with prior authentication guidance, the FFIEC Guidance emphasizes that effective risk management "may vary at financial institutions based on their respective operational and technological complexity, risk assessments, and risk appetites and tolerances."[32]

You can access the FFIEC Guidance here: https://www.fdic.gov/news/financial-institution-letters/2021/fil21055a.pdf.

LITIGATION AND ENFORCEMENT DEVELOPMENTS

Settlement Reached in Plaid Privacy Litigation

On August 5, 2021, Plaid, Inc.'s ("Plaid") and eleven named plaintiff's (the "Plaid Plaintiffs") reached a settlement (the "Plaid Settlement")[33] in the consolidated and amended class action complaint originally brought against Plaid on May 4, 2020 by the Plaid Plaintiffs in five separately-filed putative class action suits (collectively, the "Plaid Complaint").[34]

The Plaid Complaint alleged that Plaid takes advantage of its position as a fintech partner that connects user accounts to widely-used financial applications, such as Venmo, Coinbase, CashApp, and Stripe, to "acquire app users' banking login credentials and then use those credentials to harvest vast amounts of private transaction history and other financial data, all without consent."[35] The plaintiffs alleged that Plaid's use of login screens that have the "look and feel of login screens used by individual financial institutions" deceives consumers into thinking they are logging in to their

own financial institution's website when they are actually communicating their credentials to Plaid. According to the plaintiffs, "Plaid's use of bank logos and color schemes, and the overall design of the interface, are intentionally deceptive."[36]

The Plaid Settlement follows an April 30, 2021 order issued by U.S. District Judge Donna M. Ryu of the U.S. District Court for the Northern District of California denying in part and granting in part Plaid's prior motion to dismiss on procedural and substantive grounds.[37] The Plaid Settlement provides for (i) monetary relief in the form of a $58 million settlement fund for the benefit of class members and (ii) injunctive relief in form of agreements by Plaid to "(1) delete certain data from its systems; (2) inform Class Members of their ability to manage the connections made between their financial accounts and chosen applications using Plaid and delete data stored in Plaid's systems; (3) continue to include certain disclosures and features in Plaid's standard Link flow; (4) minimize the data Plaid stores; (5) enhance disclosures in Plaid's End User Privacy Policy about the categories of data Plaid collects, how Plaid uses data, and privacy controls Plaid has made available to users; and (6) continue to host a dedicated webpage with detailed information about Plaid's security practices."[38]

The case before the U.S. District Court for the Northern District of California is *In Re Plaid Privacy Litigation*, Case No. 4:20-cv-03056. You can access the docket here: https://ecf.cand.uscourts.gov/cgi-bin/iqquerymenu.pl?359040.

PayPal Announces SEC Investigation into Regulation II Issues and CFPB Investigations into Venmo Regulation E Compliance and PayPal Regulation Z Compliance

On July 29, 2021, PayPal Holdings, Inc. ("PayPal") announced in its Form 10-Q filing for the quarterly period ended June 30, 2021, that it is cooperating with the U.S. Securities and Exchange Commission's (the "SEC") Enforcement Division "relating to whether the interchange rates paid to the bank that issues debit cards bearing our licensed brands were consistent with Regulation II . . . and to the reporting of marketing fees earned from [PayPal]'s branded card program."[39] PayPal's debit card issuing bank, The Bancorp Bank, through its parent, The Bancorp, Inc., has disclosed in multiple regulatory filings that the SEC has been investigating "its card issuance activity and gross dollar volume data" since October 9, 2019.[40]

PayPal also disclosed in its Form 10-Q that it was cooperating with the Consumer Financial Protection Bureau (the "CFPB") relating to two civil investigative demands relating to (i) "Venmo's unauthorized funds transfers and collections process" and (ii) "the marketing and use of PayPal Credit in connection with certain merchants that provide educational services."[41]

You can access the PayPal 10-Q here: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001633917/000163391721000149/pypl-20210630.htm

You can access The Bancorp, Inc.'s 10-Q

here: https://www.sec.gov/ix?doc=/Archives/edgar/data/1295401/000156276221000328/tbbk-20210630x10q.htm

CFBP Files Opening Argument in Appeal Defending Prepaid Accounts Rule

On August 16, 2021, the CFPB filed an opening brief (the "Opening Brief")[42] with the U.S. Court of Appeals for the District of Columbia Circuit in its appeal of a December 2020 ruling by U.S. District Judge Richard J. Leon of the U.S. District Court for the District of Columbia that granted summary judgement in favor of PayPal Inc. and vacated two provisions of the so-called Prepaid Accounts Rule set forth in Regulation E and Regulation Z: the mandatory short-form disclosure requirement under 12 C.F.R. § 1005.18(b) and the 30-day credit linking restriction under 12 C.F.R. § 1026.61(c)(1)(iii).[43] Specifically, with respect to the short-form disclosure requirement, Judge Leon determined that the statutory authority relied on by the CFPB in promulgating the provision did not authorize the issuance of mandatory requirements regarding form, structure and content, but merely optional model forms.[44]

In the Opening Brief, the CFPB does not appeal Judge Leon's ruling with respect to the thirty-day credit linking restriction. However, the CFPB argues that its short-form disclosure requirement is entitled to deference for two reasons. First, nothing in the Regulation E's authorizing legislation, the Electronic Fund Transfer Act (the "EFTA"), "forecloses—let alone unambiguously forecloses—the CFPB from exercising its authority under EFTA to adopt requirements for the content and formatting of disclosures."[45] Second, section 1032(a) of the Dodd-Frank Act independently authorizes the short-form disclosure requirement. Section 1032(a) of the Dodd-Frank Act authorizes the CFPB to adopt rules "to ensure that the features of any consumer financial product or service . . . are fully, accurately, and effectively disclosed."[46]

The case before the U.S. Court of Appeals for the District of Columbia Circuit is *PayPal Inc. v. CFPB et al.*, Case No. 21-5057. You can access the Opening Brief here: https://ecf.cadc.uscourts.gov/n/beam/servlet/TransportRoom?servlet=CaseSummary.jsp?caseNum=21-5057&dktType=dktPublic&incOrigDkt=Y&incDktEntries=Y

CFPB Enters into Consent Order with Point of Sale Loan Originator Over Unauthorized Consumer Loans

On July 12, 2021, the CFPB entered into a consent order (the "Consent Order")[47] with GreenSky, LLC ("GreenSky") over alleged unfair acts and practices in violation of the Consumer Financial Protection Act of 2010's (the "CFPA") prohibition of unfair, deceptive, or abusive acts or practices or "UDAAPs."[48] Unfair acts or practices are those that (i) cause substantial injury to consumers, (ii) are not outweighed by any offsetting consumer or competitive benefits, and (iii) are not reasonably avoidable by consumers.[49] Specifically, the Consent Order alleges that GreenSky (i) "engaged in unfair acts and practices with regard to loans to consumers who did not authorize them" and (ii) "engaged in unfair acts and practices by structuring its loan origination

and servicing activities in a manner that enabled unauthorized loans."[50]

According to the Consent Order, GreenSky engages in loan origination and servicing activities on behalf of partner banks. GreenSky works with merchants to "market and intake loan applications from consumers at the point of sale."[51] As a part of the program, GreenSky merchants are trained on how to assist their customers in applying for GreenSky loans. Once an application is received, GreenSky performs an "on-the-spot" financing decision by comparing the application data against the lending criteria from its partner banks. Once financing is approved, the loan proceeds are distributed directly to the merchant. The consumer then receives loan packages in the mail or via email.[52]

The Consent Order alleges that between 2014 and 2019 at least 1,600 loans were fraudulently or deceptively originated. In many cases, according to the Consent Order, the merchant would apply for the loans without the consumer's knowledge. The Consent Order alleges that (i) GreenSky's processes created the opportunity for the origination of unauthorized loans, (ii) its training programs were deficient, (iii) its merchant oversight was ineffective, and (iv) its complaint resolution procedures were deficient. For example, the record shows that GreenSky received over 6,000 complaints of unauthorized loan origination and failed to stop loans that contained merchant contact information instead of consumer contact information.

Under the Consent Order, GreenSky agrees to (i) "provide up to $9 million in cash refunds and loan cancellations," (ii) pay a civil penalty in the amount of $2.5 million to the CFPB's Civil Penalty Fund, and (iii) improve its consumer identity verification, consumer complaint management program, and merchant oversight and training.[53]

You can access the Consent Order here: https://files.consumerfinance.gov/f/documents/cfpb_greensky-llc_consent-order_2021-07.pdf.

Summary Judgement Ordered in Favor of CFPB in 2017 Payday Lending Final Rule Litigation

On August 31, 2021, U.S. District Judge Lee Yeakel of the U.S. District Court for the Western District of Texas granted summary judgement in favor of the CFPB (the "SJ Order")[54] in a case in which trade organizations Community Financial Services Association of America, Ltd., and Consumer Service Alliance of Texas ("Payday Plaintiffs") continue to challenge the remaining portions of the CFPB's 2017 final rule on payday, vehicle title, and certain high-cost installment loans (the "2017 Final Rule").[55] On July 7, 2020, the CFPB issued a subsequent final rule[56] revoking the requirements of the 2017 Final Rule related to the underwriting of covered short-term and longer-term balloon-payment loans, including payday and vehicle title loans, and related reporting and recordkeeping requirements while retaining requirements and limitations, applicable to the same set of loans as well as certain high-cost installment loans, regarding attempts to withdraw payments from consumers' checking or other accounts (the "Payment Provisions").

In the SJ Order, Judge Yeakel found that the Payment Provisions of the 2017 Final Rule are "consistent with the CFPB's statutory authority and are not arbitrary and capricious."[57] The 2017 Final Rule was originally set to become effective in August 2019, however, the rule has been stayed pending the outcome of this litigation. In the SJ Order, Judge Yeakel ended the indefinite stay and set a new full-compliance date of "286 days after the date of [the SJ Order]" which is June 13, 2022.

As expected, on September 9, 2021, the Payday Plaintiffs filed a notice of appeal and simultaneously asked the court to stay the 286-day countdown until their appeal is concluded.[58]

The case before the U.S. District Court for the Western District of Texas is *Community Financial Services Association of America, Ltd. v. Consumer Financial Protection Bureau*, 2021 WL 4132272 (W.D. Tex. 2021), Case No. 1:18-cv-00295. You can access the docket here: https://ecf.txwd.uscourts.gov/cgi-bin/DktRpt.pl?530050050693702-L_1_0-1.

Consumer Advocacy Groups Sue CFPB to Enjoin Advisory Committee

On August 20, 2021, the National Association of Consumer Advocates, United States Public Interest Research Group, and Professor Kathleen Engel (collectively, "Plaintiffs") filed a motion for summary judgement (the "SJ Motion") in the United States District Court for the District of Massachusetts, in Plaintiffs' case against the CFPB alleging that the CFPB's Federal Consumer Financial Law Taskforce ("Taskforce"), which the CFPB created to improve consumer financial laws and regulations,[59] violated the Federal Advisory Committee Act ("FACA").

The SJ Motion is largely a recitation of the allegations set forth in the initial complaint (the "Complaint"). In the Complaint, the Plaintiffs alleged that the Taskforce violates the FACA by operating in secrecy and that the CFPB failed to make the "requisite findings that the Taskforce is essential and in the public interest."[60] In addition, the Plaintiffs challenged the composition of the Taskforce, alleging that its Chairman, Todd Zywicki, has described the CFPB as a "menace" and "worked on behalf of several large financial institutions to influence the CFPB and other agencies,"[61] and that "[a]ll of his fellow Taskforce members have either expressed similar views or continue to work as industry consultants or lawyers."[62]

The Plaintiffs seek complete relief, including declaratory and injunctive relief, and an order (i) setting aside the Taskforce's charter,(ii) requiring the Taskforce to make all records public, and (iii) barring the CFPB "from accepting advice or recommendations from the Taskforce."[63]

The case before the U.S. District Court for the District of Massachusetts is *National Association of Consumer Advocates et al. v. Consumer Financial Protection Bureau et al*, Case No. 1:20-cv-11141. You may access the Complaint and SJ Motion here: https://ecf.mad.uscourts.gov/cgi-bin/DktRpt.pl?567706265443371-L_1_0-1.

OFAC Settles with Payoneer for Sanctions Violations

On July 23, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") announced an agreement with Payoneer Inc. ("Payoneer") to "settle its potential civil liability for 2,260 apparent violations of multiple sanctions programs" (the "Payoneer Settlement").[64] Payoneer is an online cross-border money transmitter that provides e-wallet, virtual bank account, and prepaid access payment solutions for corporate clients. Specifically, the Payoneer Settlement states that Payoneer processed transactions totaling $802,117.36 on behalf of persons on OFAC's List of Specially Designated Nationals and Blocked Persons. The processed payments consisted of commercial transactions processed on behalf of Payoneer's corporate customers and card-issuing financial institutions. According to the Payoneer Settlement, the violative payments resulted from sanctions compliance control breakdowns, including:

> (i) weak algorithms that allowed close matches to SDN List entries not to be flagged by its filter, (ii) failure to screen for Business Identifier Codes (BICs) even when SDN List entries contained them, (iii) during backlog periods, allowing flagged and pended payments to be automatically released without review, and (iv) lack of focus on sanctioned locations, especially Crimea, because it was not monitoring IP addresses or flagging addresses in sanctioned locations.[65]

The base civil monetary penalty applicable to Payoneer is $3,889,726; however, the settlement amount of $1,400,301.40 is reflective of the total facts, including aggravating and mitigating factors. Among Payoneer's aggravating actions, OFAC highlighted Payoneer's failure "to exercise a minimal degree of caution or care for its sanctions compliance obligations" as evidenced by the fact that it had reason to know that the payments would violate sanctions based "on common indicators of location within its possession, including billing, shipping, or IP addresses, or copies of identification issued in jurisdictions and regions subject to sanctions." The reported mitigating factors include Payoneer's quick self-reporting once the violations were self-identified, no prior violations within the past five years, and improvement to its compliance programs.[66]

You can access the Payoneer Settlement here: https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf.

OFAC Settles with First Bank SA and JC Flowers & Co. Over Sanctions Violations

On August 27, 2021, OFAC announced an agreement with First Bank SA, a Romanian bank ("First Bank"), and its U.S. parent company, JC Flowers & Co. ("JC Flowers") to "settle potential civil liability for First Bank's processing of transactions in apparent violation of OFAC's Iran and Syria sanctions programs" (the "First Bank Settlement").[67] Specifically, the First Bank Settlement states that First Bank processed transactions totaling $3,589,189 on behalf of parties located in Iran and Syria.[68] The processed transactions occurred after JC Flowers acquired a majority ownership interest in First Bank in 2018.[69] The investigation into First Bank began when its regulator, the National Bank of Romania,

flagged a transaction that First Bank had processed from Romania to Syria. Thereafter, First Bank voluntarily commenced a five-year lookback in March 2019, the results of which were voluntarily disclosed to OFAC.[70] According to the First Bank Settlement, the violative transactions resulted from "First Bank's lack of understanding of the scope of U.S. sanctions regulations applicable to financial institutions without a physical presence in the United States."

The base civil monetary penalty applicable to this matter is $1,742,056, however, the settlement amount of $862,318 is reflective of the total facts, including aggravating and mitigating factors. Among First Bank's aggravating actions, OFAC highlighted (i) First Bank's "demonstrated reckless disregard for U.S. sanctions regulations," (ii) First Bank's actual knowledge of the locations of parties to the violative transactions, and (iii) the fact that the violative transactions conferred an economic benefit of over $3,589,189 to persons in Iran and Syria.[71] The reported mitigating factors included (a) First Bank's lack of violations preceding the violative transactions, (b) First Bank's cooperation with OFAC, and (c) First Bank's self-initiated renovation of its internal policies and procedures to ensure compliance with U.S. sanctions programs.[72]

You can access the First Bank Settlement here: https://home.treasury.gov/system/files/126/20210827_firstbank_flowers.pdf.

ENDNOTES:

[1]Federal Banking Agencies, *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks* (Aug. 11, 2021), https://www.occ.gov/news-issuances/news-releases/2021/nr-ia-2021-85a.pdf.

[2]OCC Bulletin 2021-40, *Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks* (Aug. 27, 2021), https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-40.html.

[3]Community Bank Fintech Guide *supra* note 1.

[4]*Id.*

[5]Board, *Community Bank Access to Innovation through Partnerships* (Sep. 2021), https://www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf.

[6]Press Release: *Federal Reserve publishes paper describing landscape of partnerships between community banks and fintech companies*, (Sep. 9, 2021), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210909a.htm.

[7]Board Governor Michelle W. Bowman, *Community Bank Access to Innovation* (Sep. 9, 2021), https://www.federalreserve.gov/newsevents/speech/bowman20210909a.htm.

[8]FinTech Partnership Paper *supra* note 5.

[9]*Id.*

[10]*Id.*

[11]*Id.*

[12]*Id.*

[13]FTC Comment Letter, *Re: Docket No. R-1748, RIN 7100-AG15, Debit Card Interchange Fees and Routing* (Aug. 11, 2021), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-board-governors-federal-reserve-system-docket-no-r-1748-rin-7100-ag15-debit-card/fed_board_staff_comment_p859910.pdf.

[14]Debit Card Interchange Fees and Rout-

ing, 86 Fed. Reg. 26,189, 26,192, 26,194 (May 13, 2021), https://www.federalregister.gov/documents/2021/05/13/2021-10013/debit-card-interchange-fees-and-routing.

[15]Press release: *Federal Reserve Board invites public comment on proposed changes to Regulation II regarding network availability for card-not-present debit card transactions and publishes a biennial report containing summary information on debit card transactions in 2019* (May 7, 2021), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210507a.htm.

[16]FTC Comment Letter *supra* note 13.

[17]*Id.*

[18]*Id.*

[19]*Id.*

[20]*Id.*

[21]*Id.*

[22]The FFIEC's membership is comprised of (i) a member of the Board, (ii) the Chairman of the FDIC, (iii) the Chairman of the National Credit Union Administration, (iv) the Comptroller of the Currency, (v) the Director of the Consumer Financial Protection Bureau, and (vi) the Chairman of the FFIEC's State Liaison Committee.

[23]FFIEC, "Authentication and Access to Financial Institution Services and Systems" (Aug. 11, 2021), https://www.ffiec.gov/press/pdf/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

[24]*Id.*

[25]*Id.*

[26]*Id.*

[27]*Id.*

[28]*Id.*

[29]*Id.*

[30]*Id.*

[31]*Id.*

[32]*Id.*

[33]*In re Plaid Privacy Litigation,* No. 3:20-cv-03056, Doc. 136 (Aug. 6, 2021).

[34]*In re Plaid Privacy Litigation,* No. 3:20-cv-03056, Doc. 61 (Aug. 5, 2020).

[35]*Id.* at 1.

[36]*Id.* at 11.

[37]*Cottle v. Plaid Inc.*, 2021 WL 1721177 (N.D. Cal. 2021).

[38]Plaid Settlement *supra* note 33.

[39]PayPal Holdings, Inc., *Form 10-Q* (Jul. 29, 2021) at 36, https://www.sec.gov/ix?doc=/Archives/edgar/data/0001633917/000163391721000149/pypl-20210630.htm.

[40]The Bancorp, Inc., Form 10-Q (Aug. 9, 2021) at 40, https://www.sec.gov/ix?doc=/Archives/edgar/data/1295401/000156276221000328/tbbk-20210630x10q.htm.

[41]PayPal Form 10-Q *supra* note 39.

[42]*PayPal Inc. v. CFPB et al.*, Case No. 21-5057, D.C. Cir. (Aug. 16, 2021) (corrected filing Aug. 18, 2021).

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

[44]*Id.* at 8-14. The EFTA requires the CFPB to "issue model clauses for optional use by financial institutions." Judge Leon concluded that this requirement also foreclosed any authority for the CFPB to mandate the form, structure and content of a disclosure.

[45]Opening Brief *supra* note 42 at 24.

[46]12 U.S.C.A. § 5532(a).

[47]*In the Matter of: GreenSky, LLC*, File No. 2021-CFPB-0004, Doc. 1 (Jul. 12, 2021), https://files.consumerfinance.gov/f/documents/cfpb_greensky-llc_consent-order_2021-07.pdf.

[48]12 U.S.C.A. § 5536(a)(1)(A).

[49]CFPB Bulletin 2013-7, *Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts* (Jul. 10,

2013), https://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf; 12 U.S.C.A. § 5531(c)(1).

[50]Consent Order *supra* note 47.

[51]*Id.*

[52]*Id.*

[53]Press Release: CFPB Takes Action Against Fintech Company GreenSky for Enabling Merchants to Secure Loans for Consumers Without Their Authorization (Jul. 12, 2021), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-fintech-company-greensky-for-enabling-merchants-to-secure-loans-for-consumers-without-their-authorization/.

[54]*Community Financial Services Association of America, Ltd. v. Consumer Financial Protection Bureau*, 2021 WL 4132272 (W.D. Tex. 2021).

[55]*Final Rule: Payday, Vehicle Title, and Certain High-Cost Installment Loans*, 82 Fed. Reg. 54,472 (Jan. 18, 2017), https://www.federalregister.gov/documents/2017/11/17/2017-21808/payday-vehicle-title-and-certain-high-cost-installment-loans.

[56]*Final Rule: Payday, Vehicle Title, and Certain High-Cost Installment Loans*, 85 Fed. Reg. 44,382 (Jul. 22, 2020), https://www.federalregister.gov/documents/2020/07/22/2020-14935/payday-vehicle-title-and-certain-high-cost-installment-loans.

[57]SJ Order *supra* note 54.

[58]*Community Financial Services Association of America, Ltd., and Consumer Service Alliance of Texas v. CFPB*, No. 1:18-cv-00295, Doc. 107 (Sep. 9, 2021).

[59]*National Association of Consumer Advocates et al. v. Consumer Financial Protection Bureau et al*, No 1:20-cv-11141, Doc. 1, 1 (D.M.A. Jun. 16, 2020).

[60]*Id.* at 3.

[61]*Id.* at 2.

[62]*Id.*

[63]*Id.* at 4.

[64]Enforcement Release: *OFAC Enters Into $1,400,301.40 Settlement with Payoneer Inc. for Apparent Violations of Multiple Sanctions Programs* (Jul. 23, 2021), https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf.

[65]*Id.*

[66]*Id.*

[67]Enforcement Release: *OFAC Enters Into $862,318 Settlement with First Bank SA and JC Flowers & Co.for Apparent Violations of Iran and Syria Sanctions Programs* (Aug. 27, 2021), https://home.treasury.gov/system/files/126/20210827_firstbank_flowers.pdf.

[68]*Id.*

[69]*Id.*

[70]*Id.*

[71]*Id.*

[72]*Id.*

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.