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

May/June 2019 ▪ Volume 22 ▪ Issue 3

ARTIFICIAL INTELLIGENCE AND FINANCE

By John Soroushian

John Soroushian is a senior policy analyst with the Bipartisan Policy Center's Financial Regulatory Reform Initiative.

The rise of artificial intelligence (AI) will change the nature of financial services. Policymakers are starting to pay attention and think of ways to adapt policy.[1] Integrating AI into the financial services sector will raise numerous challenges, requiring thoughtful assessment and flexibility as the technology evolves.

AI IN FINANCE

One model for thinking about the newest wave of AI is that of a prediction machine:[2] AI uses data to make predictions. For example, an algorithm takes medical data to predict the likelihood that a patient will have a heart attack.

AI has seen tremendous advances in recent years that have helped lower the cost and increased the accuracy of predictions. These advances have made AI more practical for business purposes in a range of industries including financial services. For instance, AI can be used for detecting credit card fraud, underwriting risk, and marketing products. These applications, if done responsibly, can improve living standards and help underserved communities better access financial services.

However, AI should not be overhyped. For example, AI is still reliant on data, so data flaws and limitations can hamper its effectiveness. AI does not substitute for human judgement in many matters either. For instance, a financial regulator still must decide what trade-offs to accept, such as whether to focus more on reducing risk or promoting innovation.

CHALLENGES

There are challenges to adapting AI in finance that need to be managed. These

IN THIS ISSUE:

THOMSON REUTERS®

42155303

challenges are often immune to simple policy solutions and sometimes require accepting difficult tradeoffs, such as striking the right balance between privacy and accuracy. Several of these challenges include:

- **Algorithmic bias:** A common misconception is that AI will be free from bias (unless the bias is deliberately hardcoded), which suggests AI could help end discrimination against protected groups. Unfortunately, this is not necessarily correct. AI can suffer from biases based on the data fed into it and design flaws that introduce (conscious or subconscious) biases of its creators. For instance, a bank that unwittingly feeds biased historical data on credit decisions to an AI will have a biased algorithm.

- **Privacy:** AI needs data to make predictions, but this raises questions about what data should be collected. More data can help improve an algorithm's predictions, but it can also intrude on people's privacy. For instance, more detailed information about an individual's purchasing habits could help improve fraud detection, but that person might not want certain information collected about their payments for medications.

- **Consumer protection:** AI raises new consumer protection concerns. For instance, an AI that is not properly designed may in effect predict that a person is prone to being duped, and target them with deceptive ads for costly and ineffective products. On the flipside, regulators might use AI to detect abuse and deception to help better tailor their regulatory efforts.

- **Overreliance:** Legendary investor Warren Buffett has said, "Beware of geeks bearing formulas."[3] Many of the most spectacular blowups in finance have resulted from overreliance and misunderstanding the limits to mathematical modeling.[4] The use of AI (which relies on mathematical modeling) is no different. AI is only as good as the data fed into it, so bad data or an unexpected event, which the AI does not have any data for, could cause its predictions to be grossly inaccurate. Not being aware of these limitations could lead to unexpected problems without proper safeguards.

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

One Year Subscription ● 6 Issues ● $ 1020.00

- **Gaming risk:** AI can be gamed. If people know their past behavior is being used to make predictions about how they will behave in the future, they may change their behavior. For instance, a study analyzed the database from an e-commerce site and found that the people who have their name in their email address were less likely to default.[5] This might suggest an email address is a good gauge of a person's credit risk. However, if people knew this was a criteria that they were going to be evaluated on, they could adapt and selectively change their email address when applying for a loan, reducing the predictive power of using an email address in making credit decisions.

- **Encouraging Responsible Innovation:** Further innovations in AI can help improve financial services, so encouraging innovation that is responsible is important. Regulatory sandboxes are programs that allow innovators to test their products with less regulatory scrutiny until they are better understood. Critics are concerned they put consumers in harm's way.[6] The design for these sandboxes and other regulatory measures can help guide the direction AI innovation takes.

FINAL THOUGHTS

The financial system is facing major changes in the way it does business. AI is giving it faster and cheaper tools to make predictions that can transform the nature of financial services. These changes can help promote stable and inclusive growth, but they can also breed instability and inequity if not managed well. Policymakers should take note and work towards a vision for AI in the financial sector that serves all.

ENDNOTES:

[1]House Financial Services Committee, Press Release: Waters Announces Committee Task Forces on Financial Technology and Artificial Intelligence, May 9, 2019, https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=403738.

[2]Agrawal, Ajay, Joshua Gans, and Avi Goldfarb. *Prediction Machines: The Simple Economics of Artificial Intelligence*. Boston, MA: Harvard Business Review Press, 2018.

[3]David Segal, *In Letter, Warren Buffet Concedes a Tough Year,* New York Times, February 28, 2009, https://www.nytimes.com/2009/03/01/business/01buffett.html.

[4]Diana B. Henriques and Joseph Kahn, ***Back from the Brink; Lessons of a Long Hot Summer***, New York Times, December 6, 1998, https://www.nytimes.com/1998/12/06/business/back-from-the-brink-lessons-of-a-long-hot-summer.html.

[5]Tobias Berg, et al., *On the Rise of FinTechs—Credit Scoring Using Digital Footprints*, FDIC Working Paper Series, September 2018, https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-04.pdf.

[6]Linda Jun, *CFPB's 'Disclosure Sandbox' Puts Consumers at Risk*, American Banker BankThink, November 19, 2018, https://www.americanbanker.com/opinion/cfpbs-disclosure-sandbox-puts-consumers-at-risk.

CLOSING THE LOOP ON PREPAID ACCESS: COMPLYING WITH FINCEN'S PREPAID ACCESS RULE IN A DIGITAL ENVIRONMENT

Jonice Gray Tucker and Brendan Clegg, Buckley LLP

Jonice Gray Tucker is a partner at Buckley LLP, specializing in working with banks, nonbank financial institutions, and other companies providing financial products and services. Brendan Clegg is an associate at the same firm.

Prepaid access vehicles have become pervasive in today's world. Among other things, such devices provide consumers with the ability to load and store funds to be used for future purchases of products and services at various vendors, facilitating efficient and convenient cash-free, and even card-free, transactions. Over the past few years in particular, there has been tremendous growth in the number and nature of retail companies offering prepaid access devices for purchases that can be made from almost anywhere in the world, through websites and mobile phone applications. For example, today's vacationing consumer can load funds into various applications via a phone, and then, order clothes to be delivered upon arrival, buy food en route, and purchase new music or audiobooks for the journey.

To keep pace with consumer demand for instant purchasing power and to expand retail reach, companies are offering novel means of using prepaid access, often in tandem with other retail partners seeking to benefit from synergies. Although many of the innovative prepaid access approaches have been pioneered by start-ups and emerging fintechs, well-established businesses, including retail giants, also are expanding their reach through creative prepaid offerings.

Many new entrants to the prepaid space are encountering a regulatory regime with which they have not had to wrestle in their existing business operations. Specifically, the Financial Crimes Enforcement Network (FinCEN), an agency of the U.S. Treasury Department, regulates "providers" and "sellers" of prepaid access as part of its oversight responsibilities for various entities covered by the Bank Secrecy Act (BSA). Despite the name, the BSA—and FinCEN's jurisdiction—are not limited to banks. The activities of many nonbank entities are regulated and the applicability of BSA requirements should be fully considered before prepaid offerings are launched, as compliance can be a time-consuming and costly endeavor.

The foundational question is whether these requirements will apply at all. Companies meeting the definition of either a "provider" or a "seller" ordinarily are covered by FinCEN's regulations. However, FinCEN has created an exemption for "closed loop" prepaid arrangements into which many companies seek to structure their operations. Determining whether a prepaid arrangement falls within this exception can be a challenging analysis, as FinCEN's guidance contains significant ambiguities. When the exception is applied to partners operating in a digital space, these ambiguities are often amplified because, in many ways, the regulatory framework has not kept pace with innovation.

Ambiguities notwithstanding, timely consideration of applicable regulations is important. Failure to comply with FinCEN's requirements,

absent cover from an applicable exception, could subject a company to potential enforcement action by the agency, including civil money penalties. Other business impacts also could be significant. Such action may draw the attention of other regulators on unrelated compliance issues. Moreover, regulatory action could result in reputational damage and attendant negative impacts on relationships with business partners and service providers. For example, service providers in the financial sector may be reticent to engage with a company that has been cited for BSA compliance deficiencies, regardless of whether those issues have been timely and fully remediated.

If issues pertaining to BSA applicability are considered early in product design, they may drive the design, enabling the company to craft a product that will not subject the company to time-consuming and costly BSA compliance enhancements, or even re-engineering. If the operations cannot be structured to fit within the exception, the company will need to undertake steps to comply with FinCEN's regulations, but at the very least, the company will be able to properly prepare for the new regulatory regime that it may face. Such steps would include allocating appropriate lead time and more fully understanding the costs that may be associated with the product.

The complex legal issues associated with application of the closed loop exception in digital environments are discussed in further detail below, and in view of the high stakes that may be associated with noncompliance, should be given careful consideration.

MEANS OF OFFERING PREPAID ACCESS

There are many potential examples where FinCEN's regulations intersect with digital products and services. They may include the following scenarios and many others:

- A company offers an app-based wallet that may be loaded with funds. The funds can be used to purchase goods at the company's brick-and-mortar locations and on its website. The funds also can be used to purchase goods at certain other entities' brick-and-mortar locations and *those* entities' websites, even though the companies are not otherwise affiliated through common ownership. The host company substantially increases brand recognition, loyalty, and may reap numerous other benefits by facilitating a streamlined payment vehicle—its application.

- A company offers an app-based wallet that may be loaded with funds. The funds may be used to purchase goods and services from the company who hosts the application as well as a network of other, unaffiliated merchants who share a common business purpose. The host company deepens customer relationships by allowing customers the ease of paying for products and services encountered at the same event (i.e., a concert), on the same trip (i.e., a vacation), or for the same type of service (i.e., restaurants).

- An online vendor selling its own products on its website offers products from separate

vendors on its website. The customer can purchase the products from the online vendor and the separate vendors using funds it loaded into a single account. From the customer perspective, purchases from the different vendors occur through one transaction. The host company benefits in ways which include customers returning to its site through purchase of products it does not produce. This setup is commonly referred to as a digital marketplace.

Whether FinCEN's regulations apply to these and similar scenarios will depend on how an individual prepaid arrangement is constructed. Areas of focus may include the number and location of participating merchants, whether the company central to the prepaid arrangement is making the parameters and details of the setup known to customers using the prepaid access devices, and the purpose underlying the arrangement.

LEGAL BACKGROUND

Overview

The BSA[1] is primarily a recordkeeping and reporting regulatory framework for covered institutions designed to provide information to law enforcement that may assist, among other things, in criminal investigations involving money laundering, terrorist financing, tax evasion, and other illicit conduct.[2] The BSA has been subject to a series of legislative enhancements since its original enactment in 1970; most recently, the USA PATRIOT Act[3] expanded the BSA's coverage to a host of nonbank financial institutions. FinCEN's implementing regulations, in turn, place substantive BSA obligations on these nonbank institutions. Among the covered institutions are money services businesses (MSBs).[4] Under FinCEN's regulations, if an entity is a "provider" or a "seller" of "prepaid access," the entity is a MSB[5] and will be subject to requirements discussed in more detail below.[6]

To determine whether compliance with FinCEN's MSB requirements is mandated, a company must first answer the threshold question of whether it is a "provider" or "seller" of prepaid access. The current prepaid access regulatory regime was implemented by FinCEN's July 2011 Prepaid Access Final Rule, which generally became effective in September 2011.[7] In issuing the Final Rule, FinCEN noted that the Rule represented an "effort to establish a more comprehensive regulatory regime over an industry in which technological advances had outpaced existing regulation."[8] Due to the maturation of the prepaid access market, the agency concluded in 2011 that prepaid access warranted commensurate BSA regulation with other MSB categories.[9] To address questions raised following the Final Rule's implementation, FinCEN issued guidance as FAQs in November 2011 (2011 FAQs)[10], and issued a supplemental set of FAQs in March 2016 (2016 FAQs) in an attempt to address recurring issues.[11]

Despite the recency of the Rule, and the supplemental guidance, the rapid pace of technological advances has continued to outpace regulation. As discussed below, this is particularly true in connection with novel prepaid access arrangements in the digital space.

Prepaid Programs and Prepaid Access

FinCEN's regulatory definitions are central to determining whether an entity is a covered "provider" or "seller" of prepaid access.[12] Both the

"provider" and, in part, the "seller" definition, depend on the existence of a "prepaid program." Without a "prepaid program," an entity will not be considered a "provider" and may be able to avoid inclusion in the definition of "seller" as well. As defined by FinCEN, a "prepaid program" is "an arrangement under which one or more persons acting together provide(s) prepaid access."[13]

A "provider" under FinCEN's regulations is the "participant *within a prepaid program* that agrees to serve as the principal conduit for access to information from its fellow program participants."[14] As relevant to this article, one way an entity can be a "seller" under FinCEN's regulations is if it "receives funds in exchange for an initial loading or subsequent loading of prepaid access" and sells that prepaid access "*offered under a prepaid program . . . .*"[15]

FinCEN's regulations specifically except several types of arrangements from the "prepaid program" definition.[16] The most relevant exception here is for closed loops: an arrangement will not be a "prepaid program" if it "provides closed loop prepaid access to funds not to exceed $2,000 maximum value that can be associated with a prepaid access device or vehicle on any day."[17] Despite FinCEN's bright-line monetary threshold, ambiguities spring from the nested term "closed loop prepaid access," defined as "access to funds or the value of funds that can be used only for goods or services in transactions involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system."[18] FinCEN further nested within *that* definition the phrase "defined merchant or location (or set of locations)," which is subject to differing interpretations that were not clarified by FinCEN at the time the phrase was introduced in 2011.[19]

Defined Merchant or Location

The Final Rule's preamble—normally a window into an agency's thinking—provides limited insight into the definition of defined merchant memorialized in the regulation. FinCEN stated in 2011 that it specifically sought to "clarify" that a "defined merchant may comprise a set of affiliated retailers or retail chains."[20] The agency explained in the preamble that during the rule drafting process, it relied on public comments from a "broad range of American retailers," who together generally advised that closed loop prepaid access was traditionally viewed as usable "within a narrowly-defined universe of entities."[21] These commenters advised that such a "narrowly-defined universe" could be composed of, for example, a group of retailers "linked by common ownership, corporate affiliation or geographic proximity."[22]

Several years later, FinCEN dedicated a FAQ to address questions regarding the term "defined merchant." In its 2016 FAQs, FinCEN indicated "defined merchant" is broader than entities linked through corporate affiliation. Specifically, "defined merchant" includes "additional unaffiliated partner merchants" joined for the "limited purpose of providing a closed loop prepaid access program."[23] The FAQ provides an example that would pass regulatory muster: a family entertainment company offers a "get-away weekend" featuring partners providing theme park admission, lodging, dining, and travel arrangements.[24] The company informs purchasers of its get-away weekend partners in media promotions, websites, and via marketing materials.[25] As a result, the

partners are identified and made known explicitly to the purchasers, and FinCEN concludes that "the standard of a 'defined merchant' has been met."[26]

This FAQ also illustrates various means by which participating merchants can be identified to consumers in closed loop arrangements. These means seemingly would include adding partners' names, logos, or trademarks on prepaid access devices themselves, in accompanying materials, or through referrals to public websites.[27] Regardless of the chosen means, FinCEN concludes that "[a]s long as the universe of merchants is identifiable and articulated to the purchasing public, and the partner merchants are joined for the limited purpose of providing a closed loop prepaid access program, such an arrangement falls within the term 'defined merchant.' "[28]

DIFFICULTIES IN APPLYING FINCEN'S DEFINITIONS TO NEW FORMS OF OFFERING PREPAID ACCESS

Since 2011, when the Final Rule was issued, commerce has moved beyond physical devices like gift cards or gift certificates, and once again, it is evident that "technological advances ha[ve] outpaced existing regulation" in this space.[29] Accordingly, even though FinCEN issued a specific FAQ relating to the scope of a "defined merchant," ambiguities remain when applying FinCEN's guidance in the context of digital marketplaces and application-based prepaid arrangements. As described below, there are open questions about: (i) the outer limits of numerical and/or geographical expansion of the definition; (ii) the standards for disclosure of participating merchants to consumers; (iii) the permissible purpose(s) of the arrangement; and (iv) the extent that the term "defined location" covers non-physical locations.

Whether a particular prepaid arrangement will qualify for the closed loop exception, ultimately, will be driven by the nuances of the arrangement's design—factors that must be carefully evaluated in view of regulatory ambiguities.

Numerical and Geographic Boundaries

The preamble to the Final Rule suggests that FinCEN struggled to demarcate where along the spectrum an arrangement would fall outside its permissible scope with respect to defined merchants or locations. It appears that at a minimum, FinCEN originally intended its exception to be somewhat limited in terms of number of merchants and relative locations. The examples listed in the regulatory definition—a retailer or chain, college campus, or subway system—are limited in either number or by geographic proximity, or both. However, the preamble's affirmation that a "defined merchant" includes a "set of affiliated retailers or retail chains" reasonably can be read to expand the numerical and geographic boundaries beyond the definition's examples.

FinCEN clarified in 2016 that permissible arrangements also could include *unaffiliated* merchants, a significant definitional expansion. Inclusion of unaffiliated merchants within a permissible closed loop could be read to imply that FinCEN's initial focus on numerical or geographic limits transitioned to a more elastic standard for determining a "defined merchant." The outer limits of a more elastic definition remain unclear, but it stands to reason that the greater the number of merchants, the more risk

that an arrangement will fall outside of the definition of a defined merchant or location.

Disclosure Methods to Consumers

The 2016 FAQs suggest that FinCEN also may consider more than numeric or geographical factors when evaluating whether a prepaid arrangement falls within the regulatory parameters. In these FAQs, FinCEN states that the "universe" of merchants must be "identifiable and articulated to the purchasing public." Accordingly, it would appear that the degree to which merchants are identified and disclosed to the public plays into the analysis of whether merchants are defined, and that such factors may even provide some cover where an arrangement includes an expansive number of merchants scattered geographically.

FinCEN delineates several methods through which it understood, as of 2016, existing merchants enumerated participating merchants or directed customers to relevant information. The space between these cited examples and the governing standard—"identifiable and articulated"—remains somewhat gray under certain factual scenarios, but the agency has provided some guideposts that provide a good starting point. The implementation of means to identify and articulate participating merchants could have significant operational impacts on the design and roll-out of a particular product or service, making this area crucial at the preliminary planning stages.

The Permissible Purposes of Such Arrangements

As noted above, FinCEN provided that so long as "the partner merchants are joined for the limited purpose of providing a closed loop prepaid access program," the defined merchant standard would be met. However, the agency has not clarified the meaning of the phrase "limited purpose" for which unaffiliated merchants must be joined. This is notable because today's merchants partner in arrangements of varying degrees of complexity, allowing participants to maximize synergies in marketing, advertising, outreach, payment processing, and product distribution, among other things. These activities go beyond mere acceptance of payments and complement what may still be the *primary* purpose of the arrangement—offering prepaid access.

Neither FinCEN's rule nor its guidance have provided a bright line on when limited purpose becomes something other than providing prepaid access, especially where an arrangement has features which maximize economies of scale and other business strengths. Making matters more complex, if the joined merchants allow payment for products and services through means other than prepaid access, would this further erode a conclusion that the merchants are aligned for the "limited purpose" of providing prepaid access?

Interpreting the phrase "limited purpose" in a manner that is unduly narrow could severely constrict business partnerships that incorporate prepaid access among a suite of benefits offered by the cooperative effort. The question, as with many other aspect of the Final Rule and FinCEN's guidance, as applied to a rapidly evolving digital world, is where the line should be drawn.

Meaning of "Defined . . . Location[s]"

Despite the focus on "defined merchant" in FinCEN's guidance, that term is not the only legal avenue to accessing the closed loop exception. FinCEN's regulatory definition of

"closed loop prepaid access" depends on access to funds used in transactions that may involve a defined merchant *or* a "defined . . . location (or set of locations)." Although on the surface this may appear to be a more straightforward path for qualifying for an exception, FinCEN has not provided any specific guidance regarding the phrase "defined . . . location (or set of locations)." Among other questions, it is unclear whether locations must be physical, or whether a "defined . . . location" could include digital locations such as websites or other electronic "locations." In today's digital environment, however, it stands to reason that electronic "locations" should be included: if a consumer views him or herself as purchasing goods from a vendor, there does not appear to be a strong argument that the purchase location's existence as a brick-and-mortar storefront or a virtual location is of importance, so long as the location is defined.

If FinCEN interpreted its definition of "closed loop prepaid access" to mean access to funds that can be used for goods or services in transactions involving a defined set of *websites*—fitting website into the regulation's term "defined location"—a company may be able to bypass the difficulties interpreting "defined merchant," a significant benefit for vendors participating in a digital marketplace concept described above.

CONSEQUENCES OF GETTING IT WRONG

As noted above, the consequences of failing to interpret the protective scope of the closed loop exception can be significant. Substantive requirements attendant to MSB status under the BSA include registration with FinCEN,[30] development and implementation of a BSA compliance program,[31] and certain reporting[32] and recordkeeping obligations.[33] An erroneous determination that the BSA does not apply—obviating MSB registration—could cause a series of derivative violations. Such an entity would not have implemented an effective BSA compliance program, filed required reports, or retained required records. FinCEN's enforcement authority for violations of its regulations includes assessment of civil penalties up to $8,249 per day for failure to register.[34] The agency can assess much higher monetary penalties for willful or grossly negligent recordkeeping violations, patterns of negligent violations of the BSA's implementing regulations, or willful violations of BSA requirements, among other things.[35]

OTHER INTERRELATED LEGAL CONSIDERATIONS

While not the focus of this article, there are several other, related legal considerations attendant to entering the prepaid access space that reinforce the need to conduct a comprehensive analysis of a proposed arrangement early in the development stages. First, if the company is involved in the acceptance and transmission of funds, it may fall within FinCEN's definition of a "money transmitter"—rendering the entity an MSB regardless of its status as a "provider" or "seller."[36] Second, companies may also have to register with state regulators under state money transmission laws, which, to varying degrees, incorporate prepaid access (or stored value), may or may not include closed loop exceptions, and may or may not track with FinCEN's language.[37]

CONCLUSION

FinCEN's issuance of new and updated guid-

ance in this space would benefit companies offering innovative prepaid access devices. As with other aspects of the BSA, the prepaid access regulations could use further modernization and supplementation to account for technological developments. Recent Congressional action and regulatory pronouncements have signaled that BSA changes may be on the horizon, but issuance of additional guidance from FinCEN on this topic is unlikely. While informal guidance from FinCEN can be requested, any responses received may not be timely to keep up with business operations, or may provide insufficient comfort to legal or compliance departments opining on the product or service offerings.

Due to the difficulty of interpreting FinCEN's guidance and the stakes involved, the best corporate strategy is to be proactive in evaluating and addressing risk. As a first step, we recommend completing a comprehensive analysis of FinCEN's regulations, as applied to the facts and circumstances of any prepaid access arrangement, and do so as early in product development as possible. Undertaking such an analysis will allow a company to determine whether there are ambiguities related to application of the closed loop exception, and if so, the magnitude of those ambiguities. Once that analysis is completed, a company can determine its level of comfort with application of the exception and the risk it is willing to take if the answer is unclear. Moreover, if an analysis is conducted at the product design phase, modifications can be implemented to the arrangement's design that may result in closer alignment with regulatory expectations, even in a regulatory environment where such ambiguities remain.

Insofar as a company seeks to rely on the closed loop exception, contemporaneous documentation of why the company concluded that the exception applies is also recommended. Documented analysis can be extremely helpful in demonstrating to regulators that thorny legal issues were considered and the company operated in good faith in relying on the exception, if the company's interpretation ultimately is challenged.

ENDNOTES:

[1]31 U.S.C.A. § 5311 *et seq.*, 12 U.S.C.A. §§ 1829b, 1951-1959.

[2]*See generally* 31 U.S.C.A. § 5311.

[3]Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of the U.S. Code).

[4]31 C.F.R. § 1010.100(t)(3).

[5] *Id.* §§ (ff)(4), (7).

[6]*See generally* 31 C.F.R. Part 1022.

[7]FinCEN, *Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access*, 76 Fed. Reg. 45403 (July 29, 2011).

[8]*Id.* at 45404. At that time, FinCEN observed that prepaid access was "becoming increasingly pervasive in American commerce, far more so than in the late 1990s when the original MSB categories were established." *Id.*

[9]*Id.*

[10]FinCEN, *Frequently Asked Questions: Final Rule—Definitions and Other Regulations Relating to Prepaid Access* (Nov. 2, 2011).

[11]FinCEN, FIN 2016-G002, *Frequently Asked Questions Regarding Prepaid Access* (Mar. 24, 2016).

[12]Prepaid access is defined as "[a]ccess to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic

serial number, mobile identification number, or personal identification number." 31 C.F.R. § 1010.100(ww).

[13]*Id.* § 1010.100(ff)(4)(iii).

[14]*Id.* § (ff)(4)(i) (emphasis added).

[15]*Id.* § (ff)(7)(i) (emphasis added). Separately, an entity can be a "seller" if it sells prepaid access to funds that exceed $10,000 to any person during any one day and the company "has not implemented policies and procedures reasonably adapted to prevent such a sale." *Id.* § (ff)(7)(ii). Importantly, this definition does not depend on the definition of "prepaid program." In fact, the definition specifically notes that the sales to funds that exceed $10,000 that cause an entity to fall into this definition can "include[e] closed loop prepaid access."

[16]*See generally id.* § (ff)(iii).

[17]*Id.* § (ff)(iii)(A). The monetary threshold for the exception is straightforward, setting a maximum dollar amount; FinCEN's 2011 FAQs explained that this threshold attaches to each device or vehicle, and companies need not aggregate separate devices or vehicles bought by an individual in a single day. 2016 FAQs, at 6. However, FinCEN also clarified that if the prepaid arrangement permits individual or cumulative reloads on a device or vehicle that, in total, allow more than $2,000 on that device or vehicle, the arrangement no longer qualifies for the exception. *Id.*

[18]31 C.F.R. § 1010.100(kkk).

[19]We note that a separate exception to FinCEN's definition of "prepaid program" may be available if a company is willing to limit its arrangement to domestic use and permit only depository sources for loading funds into user's accounts, among other limitations, but this article does not address that separate exception in detail because such structural limitations may inhibit the usability and convenience of a prepaid access arrangement. *See id.* § (ff)(4)(iii)(D). Under this exception, the arrangement must provide prepaid access solely to funds "not to exceed $1,000 maximum value and from which no more than $1,000 maximum value can be initially or subsequently loaded, used, or withdrawn on any day through a device or vehicle," and cannot permit (i) funds or value to be transmitted internationally, (ii) transfers between or among users of prepaid access within a prepaid program, or (iii) loading additional funds or the value of funds from non-depository sources.

[20]*See* 76 Fed. Reg. at 45413.

[21]*See id.* at 45407.

[22]*See id.*

[23]2016 FAQs.

[24]*Id.*

[25]*Id.*

[26]*Id.*

[27]*Id.*

[28]*Id.*

[29]76 Fed. Reg. at 45404.

[30]31 C.F.R. § 1022.380.

[31]*Id.* § 1022.210(a).

[32]*See, e.g.*, *id.* § 1022.320 (setting out procedures for filing suspicious activity reports with FinCEN).

[33]*See, e.g.*, *id.* § 1022.420 (setting out record-keeping requirements for providers to maintain access to certain transactional records generated in the ordinary course of business that would be needed to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers, and other prepaid-related transactions).

[34]*See* 31 U.S.C.A. § 5330(e); 31 C.F.R. 1010.821(b), Table 1.

[35]*See* 31 C.F.R. 1010.821(b), Table 1.

[36]*See id.* § 1010.100(ff)(5).

[37]*See, e.g.*, Cal. Fin. Code § 2003(q) (defining "money transmission" to include, among other things, "selling or issuing stored value").

FINTECH LAW REPORT: MAY/JUNE 2019 REGULATION AND LITIGATION UPDATE

By Duncan Douglass and Amanda Mollo

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

REGULATORY DEVELOPMENTS

New York Federal Reserve Bank Launches "Fintech Advisory Group"

On April 1, 2019, the 10 members of a new "Fintech Advisory Group" group formed by the Federal Reserve Bank of New York met for the first time. The group will meet twice annually for discussions aimed at taking a more active approach toward emerging fintech issues.

According to a press release announcing its launch, the "primary goal" of the Fintech Advisory Group is "to present views and perspectives on the emerging issues related to financial technologies, the application and market impact of these technologies, and the potential impact on the New York Fed's ability to achieve its missions," and to "provide Bank leaders with a high-level platform to establish clear points of contact with senior representatives and thought leaders from the financial technology industry and consumer organizations."[1] The Fintech Advisory Group members include attorneys, bankers and academics, and the group plans to consider how training, hiring and interactions within the market can keep pace with new financial technologies. Each of the members will serve on the group for terms of two years on a rotational basis, and members are selected based on their expertise relevant to financial technologies.

The members of this advisory group are Gary Gensler, former chairman of the Commodity Futures Trading Commission; Martin Fleming, chief analytics officer at IBM; Ulku Rowe, director of financial services at Google Cloud; Patrick Murck, special counsel at Cooley LLP; Andrew Boyajian, head of banking at TransferWise; Lee Braine of the chief technology office at Barclays; David Waller, a partner and head of data science at Oliver Wyman consulting firm; Michael Bodson, chief executive officer at the Depository Trust & Clearing Corporation; Lena Mass-Cresnik, chief data officer at Moelis & Company investment bank; and Sonal Shah, executive director of the Beeck Center for Social Impact and Innovation.

You can read the Fintech Advisory Group charter here:

https://www.newyorkfed.org/medialibrary/media/aboutthefed/pdf/FinTech-Charter.pdf

OCC Requests Comment on Fintech Pilot Program

On April 30, 2019, the Office of the Comptroller of the Currency ("OCC") published plans for a new program (the "Pilot Program") through its Office of Innovation that would allow entities subject to OCC supervision, such as nationally chartered banks and their third-party service providers, to work closely with the OCC to test "new or unique activities where uncertainty is perceived to be a barrier to development and implementation."[2] Through a press release, which was accompanied by a paper describing the Pilot Program and a separate Frequently Asked Questions document, the OCC announced that it was

opening a 45-day comment period and seeking feedback on "all aspects" of the Pilot Program, from whether the Pilot Program would provide additional value to more granular details about the eligibility criteria for participation.[3]

According to the OCC, eligible entities would be able to propose a pilot individually, in conjunction with a third party, or as a collaborative effort among multiple banks; but third parties would not be permitted to submit a proposal independently. Prior to submitting a formal "expression of interest" in the Pilot Program to the Office of Innovation or to the entity's assigned supervisory office, the OCC would encourage entities to engage in informal dialogue with the regulator to receive "informal feedback and for interested parties to gain a deeper understanding of the program's structure and OCC expectations."[4] Formal expressions of interest, which should be tailored to the scope and complexity of the entity's proposed activities, would be expected to describe the proposed activity, including its objectives, duration, intentions for OCC involvement, safeguards to prevent and control any adverse outcomes, and exit strategy, among other things. The OCC would review requests on a case-by-case basis. If a proposal was accepted, the OCC would permit the entity to engage in its proposed activity in a controlled manner through the Pilot Program for a period no less than three months but no greater than two years. The OCC would use a variety of regulatory tools, such as interpretive letters, supervisory feedback, and technical assistance from the OCC's subject matter experts, to assist participating entities throughout the Pilot Program. Unlike other recent efforts by regulators to embrace fintech innovation (*e.g.*, regulatory "sandboxes"), the Pilot Program would not offer a safe harbor from consumer protection requirements or any immunity from federal or state enforcement actions.

The OCC said the proposed Pilot Program is separate from the new fintech chartering process, and participants in the new program do not get an "expedited path" to a national bank charter.

Comments on the proposed program should be submitted by June 14, 2019. You can read the Pilot Program materials here:

https://occ.treas.gov/news-issuances/news-releases/2019/nr-occ-2019-42.html;

https://occ.treas.gov/topics/responsible-innovation/occ-innovation-pilot-program.pdf;

https://occ.treas.gov/topics/responsible-innovation/occ-innovation-pilot-program-faqs.pdf.

FinCEN Issues Guidance Summary for Virtual Currency Industry

On May 9, 2019, the Financial Crimes Enforcement Network ("FinCEN") issued guidance entitled "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies [('CVCs')]" (the "Guidance"). The stated purpose of the Guidance is to "remind persons subject to the Bank Secrecy Act ('BSA') how FinCEN regulations relating to money services businesses ('MSBs') apply to certain business models involving money transmission denominated in value that substitutes for currency" and to "help financial institutions comply with their existing obligations under the BSA as they relate to current and emerging business models involving CVC."[5] Accordingly, the Guidance "does not establish any new regulatory expectations or requirements," but consolidates

current FinCEN regulations, administrative rulings, and guidance and demonstrates how those rules and interpretations apply to common business models involving CVCs engaging in "the same underlying patterns of activity."[6]

You can read the Guidance here:

https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models.

LITIGATION AND ENFORCEMENT DEVELOPMENTS

FinCEN Announces First Enforcement Action against Peer-to-Peer Virtual Currency Exchange

On April 18, 2019, FinCEN published its first enforcement action against a peer-to-peer virtual currency exchanger, Eric Powers of Kern County California. According to the Assessment of Civil Money Penalty (the "Assessment") issued by FinCEN, Mr. Powers admits that he violated the BSA's registration, program, and reporting requirements from December 6, 2012 through September 24, 2014 when he "failed to: (a) register as an MSB with FinCEN; (b) establish and implement an effective written AML program; (c) detect and adequately report suspicious transactions; and (d) report currency transactions."[7] Mr. Powers was required to register as an MSB with FinCEN because he operated as a peer-to-peer exchanger of convertible virtual currency and thus was a money transmitter required to comply with the BSA obligations that apply to MSBs, which also include developing, implementing, and maintaining an effective AML program; filing Suspicious Activity Reports ("SARs") and Currency Transaction Reports ("CTRs"); and maintaining certain records.

According to the Assessment, a peer-to-peer exchanger is "a natural person engaged in the business of buying and selling convertible virtual currency, who typically advertises and markets his or her services through classified ads, specifically designed web platform websites, online forums, other social media, and word of mouth."[8] In the press release accompanying the publication of the Assessment, FinCEN Director Kenneth A. Blanco stated that "[o]bligations under the BSA apply to money transmitters regardless of their size," and that it "should not come as a surprise" that FinCEN would bring an enforcement action against a peer-to-peer exchanger in accordance with previously issued agency guidance.[9] Nevertheless, FinCEN acknowledged that "this is its first enforcement action against a peer-to-peer virtual currency exchanger and the first instance in which it has penalized an exchanger of virtual currency for failure to file CTRs."[10]

According to the Assessment and accompanying press release, Mr. Powers' conduct was particularly egregious in that "there were indications that Mr. Powers specifically was aware of [his BSA] obligations, but willfully failed to honor them," and he conducted "numerous suspicious transactions without ever filing a SAR" and "over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single CTR."[11] In particular, Mr. Powers conducted over 150 separate in-person cash transactions for over $10,000 with a single individual and paid approximately $60,000 in cash to another customer.[12] Similarly, "[a]s a money transmitter, Mr. Powers processed transactions

that bore strong indicia of illicit activity," including over one hundred transactions on the darknet website Silk Road and a particular offer to exchange CVC for fiat currency that Mr. Powers knew constituted the proceeds of illegal activity.[13] Nevertheless, Mr. Powers never filed a SAR, and he failed to maintain adequate records of these suspicious transactions.

In addition to paying a $35,000 fine, Powers agreed to an industry bar that would prohibit him from providing money transmission services or engaging in any other activity that would make him an MSB for purposes of FinCEN regulations.

You can read the Assessment here:

https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf.

FTC Permanently Bans Payment Processor for Failing to Comply with 2009 Order Requiring Monitoring Of Merchant Clients

On April 10, 2019, the Federal Trade Commission ("FTC") entered into a settlement (the "Settlement") with Thomas Wells and payment processor Priority Payout Corp. ("Priority"), a successor entity to InterBill, Ltd. ("InterBill"), permanently banning Mr. Wells and Priority from engaging in, and assisting others with, payment processing, and assessing a $1.8 million contempt judgment against them. The Settlement alleges that Mr. Wells and Priority repeatedly violated a court order issued against Wells and InterBill in 2009 (the "2009 Order").

In 2006, the FTC had filed a complaint against Mr. Wells and InterBill, alleging that InterBill had "debited, or tried to debit, more than $9.9 million from consumers' bank accounts without those consumers' authorization . . . in connection with providing payment processing services to a fraudulent enterprise known as Pharmacycards.com."[14] As a result of the 2006 Complaint, the FTC entered into the 2009 Order with Mr. Wells and InterBill, assessed a fine for over $1.7 million, and required both Mr. Wells and InterBill to "more carefully review and monitor their merchant-clients, and prospective merchant-clients, to ensure the merchants were not engaged in deceptive or unfair practices."[15]

According to the recent Settlement, Mr. Wells and Priority (InterBill's successor company) do not contest that the FTC could submit sufficient evidence to demonstrate that they "violated the 2009 Order by providing and procuring payment processing for merchant-clients engaged in fraud, failing to conduct a reasonable investigation of prospective merchant-clients, and failing to monitor merchant-clients' transaction activity to ensure that the client is not engaged in practices that are deceptive, unfair, or abusive."[16] As a consequence, Mr. Wells and Priority are subject to new fines and the ban on engaging in payment processing described above.

You can read the Settlement here:

https://www.ftc.gov/system/files/documents/cases/interbill_final_order_as_to_tom_wells.pdf.

NYDFS Fintech Charter Suit against OCC Survives Motion to Dismiss

On May 2, 2019, the U.S. District Court for the Southern District of New York denied the OCC's February 26 motion to dismiss a complaint filed by the New York Department of Financial Services ("NYDFS") disputing the agency's authority to grant special purpose na-

tional bank charters to fintech companies. The NYDFS challenged the OCC fintech charter on the grounds that (i) the OCC lacks the statutory authority to charter non-depository entities; (ii) the OCC's promulgation of regulation 12 C.F.R. § 5.20(e)(1), permitting the OCC to issue special purpose national bank charters, exceeded its statutory authority, which limits the OCC to chartering entities that carry on the business of banking; (iii) the OCC's decision to grant fintech charters failed to comply with the rulemaking requirements of the National Bank Act ("NBA"); (iv) the OCC's decision to issue fintech charters is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; and (v) the OCC's decision to grant fintech charters to fintech companies violates the Supremacy Clause and the Tenth Amendment by preempting otherwise applicable state law without statutory authority.

The OCC had argued that the court should dismiss the NYDFS's complaint because the NYDFS cannot suffer an injury in fact and thus have standing to sue until the OCC approves an application for a fintech charter and the OCC has not yet received an application for a fintech charter. The OCC also disputed the assertion that its announcement that it will accept applications for fintech charters is arbitrary and capricious. Rather, the OCC argued that the core issue is not the 2018 fintech charter announcement, but the OCC's 2004 special purpose bank regulation, 12 C.F.R. § 5.20(e)(1). As such, the OCC contended that the NYDFS's claim is time-barred. The OCC also asserted that its July 2018 announcement was not a final agency action, and thus is not subject to judicial review under the Administrative Procedure Act.

U.S. District Judge Victor Marrero found that the NYDFS claims were "both constitutionally and prudentially ripe for adjudication" because "early action by state plaintiffs to combat concerns arising from unlawful federal agency action can be warranted," drawing on comparisons to similar controversies between states and the federal government.[17] Judge Marrero also noted that the NYDFS "benefits from the supposition that the government enforces and acts on its recent, non-moribund laws."[18] Indeed, the NYDFS had argued that its case is now ripe partly because Comptroller of the Currency Joseph Otting has repeatedly said the OCC has met with hundreds of fintechs and one is soon to apply for the charter. Judge Marrero found that, "[i]n light of these expectations, [the NYDFS] has demonstrated a 'substantial risk that the harm will occur' " and that the NYDFS "faces the current risk that entities may, at any moment, leave its supervision to seek greener pastures," placing New York citizens at risk.[19]

With respect to the NYDFS's statutory challenge under the NBA, the court was not persuaded by the OCC's argument that it is entitled to deference under the standards set forth in *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*,[20] due to ambiguities inherent in the NBA. Judge Marrero found that "the term 'business of banking,' as used in the NBA, unambiguously requires receiving deposits as an aspect of the business."[21] In support of this conclusion, Judge Marrero points to the historical meaning of "banking" at the time of the NBA's passage, the OCC's longstanding practice of chartering only depository entities as national banks unless Congress first amended the NBA explicitly to authorize the OCC to charter other entities, and "the canon of construction under which the plausibility of an agency interpretation

of statutory text that would confer new power upon that agency bears inverse relation to the size of that putative power and the belatedness of the putative discovery."[22]

However, the court dismissed the NYDFS's claims that a fintech charter conflicts with state law in violation of the Tenth Amendment of the U.S. Constitution. According to the court, the NYDFS has failed to state such a Tenth Amendment claim "because federal law preempts state law only when 'Congress has clearly expressed its intent,' " and in this instance, "the operative question is not whether the federal government has the power to take the action challenged in this case, but whether Congress has, in fact exercised that power."[23]

While the NYDFS case against the OCC will now proceed, another OCC motion to dismiss is currently pending in the lawsuit filed by the Conference of State Bank Supervisors in the United States District Court for the District of Columbia to block the OCC from issuing fintech charters.

The case before the U.S. District Court for the Southern District of New York is *Vullo v. Office of the Comptroller of the Currency et al.*, No. 1:18-cv-08377. You can read the Decision and Order here:

https://ecf.nysd.uscourts.gov/doc1/127124666317.

RD Legal Funding Case Brings CFPB Constitutionality Issue to Second Circuit

On March 15, 2019, the Consumer Financial Protection Bureau ("CFPB") and New York Attorney General ("NYAG"), filed briefs with the Second Circuit in their separate appeals challenging Chief District Judge Loretta A. Preska's dismissal of their lawsuit against a group of defendants who offered cash advances to consumers waiting on payouts from legal settlement agreements or judgments, alleging violations of the Consumer Financial Protection Act (the "CFPA") and New York law.

In September, Judge Preska dismissed[24] all of the NYAG's federal and state law claims, explicitly ordering that the NYAG's claims under Dodd-Frank Section 1042 were dismissed "with prejudice" and that the NYAG's remaining state law claims should be heard in state court, in both cases following her June 21, 2018 order[25] ruling that the CFPB's structure is unconstitutional and that the proper remedy would be to strike down Title X of the Dodd-Frank Act, the CFPA, in its entirety.

Both the CFPB and NYAG's primary argument on appeal is that the CFPB's structure, including the for-cause requirement to remove the CFPB director, is constitutional. Specifically, the briefs discuss the precedents that establish Congress' authority to protect independent agency heads from removal except for cause and that the for-cause removal structure does not impede the president in performing constitutional duties. In the alternative, both appellants argue that the proper remedy, in the event that the Second Circuit determines that the Dodd-Frank Act's for-cause removal provision is unconstitutional, would be to sever that provision rather than strike down the entire CFPA, as Judge Preska did. The NYAG also argues that Judge Preska erred in dismissing all of its federal law claims with prejudice because the NYAG claims against the defendants implicate the Anti-Assignment Act, a federal law that prohibits the assignment of

federal awards, and thus the NYAG claims incorporate a federal question even if the Second Circuit affirms Judge Preska's ruling that the CFPB is unconstitutionally structured and the only remedy is to strike down the CFPA.

The case before the Second Circuit is *CFPB v. RD Legal Funding, LLC*, No. 18-2743. The appellants' briefs are available here:

https://ecf.ca2.uscourts.gov/n/beam/servlet/TransportRoom.

CFPB Structure Held Constitutional by Ninth Circuit Court of Appeals

On May 6, 2019, the U.S. Court of Appeals for the Ninth Circuit unanimously held that the CFPB's single-director structure is constitutionally permissible. The unsuccessful challenge to the CFPB's constitutionality was brought by a debt collection law firm, Seila Law LLC, in an attempt to challenge a CID that was part of a CFPB investigation into whether Seila Law had violated the Telemarketing Sales Rule in its marketing of debt relief services. Seila Law's main argument was that the CFPB is unconstitutionally structured because "an agency with the CFPB's broad law-enforcement powers may not be headed by a single Director removable by the President only for cause."[26] The firm also challenged the CID as violating the practice-of-law exclusion in the Consumer Financial Protection Act.

Writing for the unanimous panel, Judge Paul Watford explained that the Supreme Court's separation-of-powers decisions in *Humphrey's Executor v. United States*[27] and *Morrison v. Olson*[28] were controlling precedent in favor of the CFPB's constitutionality.[29] According to the Ninth Circuit panel, those cases indicate that it is permissible for Congress to require quasi-legislative and/or quasi-judicial agencies to discharge their duties independently of executive control,[30] and that the for-cause removal restriction protecting the CFPB's Director does not "impede the President's ability to perform his constitutional duty" to ensure that the laws are faithfully executed.[31]

The court also rejected Seila Law's challenge to the CFPB's investigative demand because the CID fit within an exception to the practice-of-law exclusion specific to the CFPB's enforcement of the Telemarketing Sales Rule.[32]

The case before the U.S. Court of Appeals for the Ninth Circuit was *CFPB v. Seila Law, LLC*, No. 17-56324. You can read the Ninth Circuit's decision here:

http://cdn.ca9.uscourts.gov/datastore/opinions/2019/05/06/17-56324.pdf.

ENDNOTES:

[1]Press release, *New York Fed Launches Fintech Advisory Group* (Mar. 22, 2019), https://www.newyorkfed.org/newsevents/news/aboutthefed/2019/20190322.

[2]Office of the Comptroller of the Currency, *OCC Innovation Pilot Program*, 3 (Apr. 30, 2019) https://occ.treas.gov/topics/responsible-innovation/occ-innovation-pilot-program.pdf.

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

[4]*Id.* at 5.

[5]Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, 1 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[6]*Id.*

[7]FinCEN, Assessment of Civil Penalty against Eric Powers, 2 (Apr. 18, 2019), https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf.

[8]*Id.* at n. 6.

[9]FinCEN, Press release*: FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws*, (Apr. 18, 2019), https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money.

[10]*Id.*

[11]*Id.*

[12]Assessment at 7.

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

[14]*Federal Trade Commission v. InterBill, Ltd. And Thomas Wells,* 2:06-cv-01644, Complaint, 3 (Dec. 26, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2007/01/070108cmp0423192.pdf.

[15]FTC, Press release: Payment Processor and Owner Agree to Permanent Payment Processing Ban and $1.8 Million Judgment to Settle FTC Charges They Violated 2009 Order, (Apr. 11, 2019), https://www.ftc.gov/news-events/press-releases/2019/04/payment-processor-owner-agree-permanent-payment-processing-ban-18.

[16]*Federal Trade Commission v. InterBill, Ltd. And Thomas Wells,* 2:06-cv-01644, Settlement, 2 (Apr. 10, 2019).

[17]*Vullo v. Office of the Comptroller of the Currency et al.*, No. 1:18-cv-08377, 24 (May 2, 2019).

[18]*Id.* at 25 (citing *Hedges v. Obama*, 724 F.3d 170, 197, 41 Media L. Rep. (BNA) 2221 (2d Cir. 2013)).

[19]*Id.* at 26.

[20]*Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 104 S. Ct. 2778, 81 L. Ed. 2d 694, 21 Env't. Rep. Cas. (BNA) 1049, 14 Envtl. L. Rep. 20507 (1984).

[21]*Vullo* at 38.

[22]*Id.* at 45-46.

[23]*Id.* at 55.

[24]*CFPB v. RD Legal Funding, LLC*, No. 17-cv-890 (S.D.N.Y. Sept. 12, 2018).

[25]*CFPB v. RD Legal Funding, LLC*, No. 17-cv-890 (S.D.N.Y. June 21, 2018).

[26]*CFPB v. Seila Law, LLC*, No. 17-56324, 5, (9th Cir. May 6, 2019).

[27]*Humphrey's Ex'r v. U.S.*, 295 U.S. 602, 55 S. Ct. 869, 79 L. Ed. 1611 (1935).

[28]*Morrison v. Olson*, 487 U.S. 654, 108 S. Ct. 2597, 101 L. Ed. 2d 569 (1988).

[29]*Seila Law* at 8.

[30]*See Humphrey's Executor*, 295 U.S. at 629.

[31]*Morrison,* 487 U.S. at 691.

[32]*Seila Law* at 9.

LETTER FROM THE EDITOR

Katie Wechsler

In this issue of *Fintech Law Report*, experts explore a variety of issues tied to the significant developments in technology.

John Soroushian, a senior policy analyst with the Bipartisan Policy Center explores the rise of artificial intelligence and its impact on the nature of financial services. Mr. Soroushian examines AI as a prediction machine, and while there are significant benefits in the advancement of AI, including more effectively combatting fraud, there are significant challenges that must be addressed. This article explores some of the key challenges including algorithmic bias, privacy, consumer protection, overreliance, gaming risk, and encouraging responsible innovation. Mr. Soroushian's approach to these challenges is worth noting: "These challenges are often immune to simple policy solutions and sometimes require accepting difficult tradeoffs, such as deciding whether we want more privacy or accuracy." As he rightly concludes:

> The financial system is facing major changes in the way it does business. AI is giving it faster and cheaper tools to make predictions that can transform the nature of financial services. These changes can help promote stable and inclusive growth, but they can also breed instability and inequity if not managed well. Policymakers should take note and work towards a vision for AI in the financial sector that serves all.

Also in this issue, Jonice Gray Tucker and Brendan Clegg of Buckley LLP dive into the fast growing market of prepaid access. Many of those in that market, particularly those that are considered either a "provider" or a "seller" of prepaid access must comply with FinCEN's BSA requirements, which is a time-consuming and costly endeavor. In their article, Ms. Tucker and Mr. Clegg explore the complex legal issues associated with the application of an exemption from these rules for "closed loop" prepaid arrangements. As the authors note, since FinCEN's rules were issued, technological advances have outpaced existing regulations, creating ambiguities and open questions about several aspects of that exemption. In addition, the authors wisely note that:

> If issues pertaining to BSA applicability are considered early in product design, they may drive the design, enabling the company to craft a product that will not subject the company to time-consuming and costly BSA compliance enhancements, or even re-engineering. If the operations cannot be structured to fit within the exception, the company will need to undertake steps to comply with FinCEN's regulations, but at the very least, the company will be able to properly prepare for the new regulatory regime that it may face. Such steps would include allocating appropriate lead time and more fully understanding the costs that may be associated with the product.

For those in the prepaid access market or considering entering that market, this article is a must-read.

Finally, Douglass Duncan and Amanda Mollo of Alston & Bird, LLP provide a comprehensive and thorough review of recent regulatory and litigation developments in fintech. There are rapid and frequent developments at both the state and federal level that have broad implications for fintech, and the authors did an excellent job at highlighting the most significant developments.

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.