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

May/June 2018 ▪ Volume 21 ▪ Issue 3

BOTS IN THE FINTECH INDUSTRY

by Lex Sokolin and Huu Nguyen

Lex Sokolin directs FinTech strategy at Autonomous Research, a global research firm for the financial sector, helping clients understand and leverage innovation, www.autonomous.com. Huu Nguyen is a partner at the international law firm of Squire Patton Boggs (US) LLP, focusing on commercial and corporate transactions in the technology space, and in particular, artificial intelligence law, www.squirepattonboggs.com.

1. Bots, Bots Everywhere

Fintech bots range from robo-advisors to customer service chat bots. Bots are ostensibly robots that operate in virtual space on behalf of people. Bots do things, like execute financial transactions, or convey information such as account balances on behalf of people. Bots are powered by artificial intelligence and range from simple programs that are pre-programed with scripts to adaptive bots that react to new situations and respond with increasing sophistication. Robo-advisors, for example may use algorithms to perform financial planning services with little to no human supervision.[i]

The power of conversational interfaces reaches across the range of Fintech industries. In Sokolin's #Machine Intelligence & Augmented Finance[ii], he writes that customer preferences for the use of people or technology is starkly divided among generational lines, with 90% of the Silent Generation (born 1925-1945) having a preference towards human service over the phone, while only 12% of Millennials prefer phone, with nearly all others looking for chat, social, or text channels. Conversational interfaces are powered by natural language processing, and there is a rich ecosystem of startups working on the client experience across banking, payments, investments and insurance, leveraging platforms like Amazon Echo and Facebook Messenger.[iii] Moreover, Fintech chatbot platforms can be consumer facing as direct distribution channels, as well as private label platforms

IN THIS ISSUE:

THOMSON REUTERS®

42023369

for banks and financial institutions to more cheaply serve their customers.[iv] There are numerous Financial chatbot in the conversational interface ecosystem. For example, IBM offers Watson financial services.[v] In another example, finn.ai company provides banks with a chatbot technology that integrates into core processors and conversational apps (e.g., Messenger), and uses a rule-based agent, making decisions based on a given set of scenarios.[vi]

As the use of bots in Fintech abounds, this begs the question of, what recent U.S. legal development and industry standards apply to the use of Fintech bots and what are the best practices for their use to minimize financial regulatory risk.

2. The Law of Bots

a. SEC Guidance on Robo-Advisors

One type of Fintech bots is the robo-advsior that provide investment advice. The Investment Advisers Act of 1940, which defines "investment adviser" in the following manner:

> (11) "Investment adviser" means any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities . . .[vii]

Investment advisors are a "fiduciary" to their advisory clients. This means that they have a fundamental obligation to act in the best interests of their clients and to provide investment advice in their clients' best interests.[viii] Some commentators have questioned whether bots can be investment advisors.[ix] Nonetheless, the Securities and Exchange Commission ("SEC") has provided substantial guidance on robo-advisors.[x] The guidance focuses on three distinct areas identified, listed below, and provides suggestions on how robo-advisers may address them:

— The substance and presentation of disclosures to clients about the robo-adviser and the investment advisory services it offers;

— The obligation to obtain information from clients to support the robo-adviser's duty to provide suitable advice; and

— The adoption and implementation of effective compliance programs reasonably de-

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

One Year Subscription ● 6 Issues ● $ 1020.00

signed to address particular concerns relevant to providing automated advice.

The recommendation requires the bot to provide "questionnaire eliciting sufficient information to allow the robo-adviser to conclude that its initial recommendations and ongoing investment advice are suitable and appropriate for that client based on his or her financial situation and investment objectives." The recommendation states that information a robo-adviser should consider providing includes among other things: a statement that an algorithm is used to manage individual client accounts; a description of the algorithmic functions used to manage client accounts (e.g., that the algorithm generates recommended portfolios; that individual client accounts are invested and rebalanced by the algorithm); and a description of the assumptions and limitations of the algorithm used to manage client accounts (e.g., if the algorithm is based on modern portfolio theory, a description of the assumptions behind and the limitations of that theory).

b. FINRA Report on Digital Investment Advice

In addition to the SEC's guidance, the Financial Industry Regulatory Agency ("FINRA"), the financial industry's self-regulatory organization, issued a Report on Digital Investment Advice.[xi] The report states:

> FINRA issues this report to remind broker-dealers of their obligations under FINRA rules as well as to share effective practices related to digital investment advice, including with respect to technology management, portfolio development and conflicts of interest mitigation. The report also raises considerations for investors in evaluating investment advice derived entirely or in part from digital investment advice tools.

The report focuses on governance and supervision in two areas: 1) the algorithms that drive digital investment tools; and 2) the construction of client portfolios, including potential conflicts of interest that may arise in those portfolios. Firms should assess whether an algorithm is consistent with the firm's investment and analytic approaches. Firms should also establish governance and supervision structures and processes for the portfolios digital investment tools may present to users. Moreover, the report states that Customer profiling functionality is a critical component of digital advice tools because it drives recommendations to customers. The financial professional-facing tools FINRA observed could be used to gather a broad range of information about a customer. Risk tolerance is another important consideration in developing a customer profile and an investment recommendation. The bot should be able reconcile inconsistent responses from customers. The report notes that this can be done through discussions with the customer or, in a purely digital environment, by making a customer aware of contradictory responses and asking additional questions to resolve the inconsistency. The report also notes the importance of rebalancing, training and education of financial professionals on the usage of bots.

c. UETA and E-Sign Act[xii]

In addition to digital investment advice, Fintech bots may perform other financial functions, including entering into automated transactions. Bots can be considered electronic agents for people and businesses. The electronic Signatures in Global and National Commerce Act ("E-Sign Act")[xiii] and the Uniform Electronic Transactions Act ("UETA")[xiv]which has been enacted 47 states[xv] permit international electronic commerce.

As the Federal Trade Commission ("FTC") succinctly stated:

> [The E-Sign Act] signed into law on June 30, 2000, provides a general rule of validity for electronic records and signatures for transactions in or affecting interstate or foreign commerce. The E-Sign Act allows the use of electronic records to satisfy any statute, regulation, or rule of law requiring that such information be provided in writing, if [a party] has affirmatively consent.

Moreover, Section 14 of the UETA permits automated transactions. Section 2(1) and (6) are relevant:

> (2) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
>
> (6) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

Also, Section 14 (1) and (2) describes the formation which can be thought of the meeting of the minds of the electronic agents:

> (1) A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.
>
> (2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

One open legal question related to using more advanced artificial agents, is whether a bot that behaves in unexpected ways or adapts to a situation not anticipated by the designer or company running the bot can be considered to have entered into an automated transaction - whether actual consent has been provided by a party under contract common law. To the authors' knowledge, no court has yet ruled on this issue.

d. Bot Speech

In a murder investigation in Arkansas, police sought certain records of interactions with a home owner's bot, Alexa[xvi] which were stored on Amazon's servers. This case involved Fourth Amendment and First Amendment arguments for the protections of bot data. In the state's search warrant[xvii], the police sought "certain records, namely electronic data in the form of audio recordings, transcribed records, or other text records related to communications and transactions between an Amazon Echo device.. that was located at James A. Bates' residence . . . and Amazon.com's services and other computer hardware maintained by Amazon.com." Amazon moved to quash the search warrant asking the court[xviii]:

> Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials. Accordingly, Amazon asks this Court, consistent with the rulings of many other courts, to require the State in the first instance to make a heightened showing of relevance and need for any recordings. Specifically, the State must demonstrate: (1) a compelling

> need for the information sought, including that it is not available from other sources; and (2) a sufficient nexus between the information and the subject of the criminal investigation.

Amazon argued[xix] among other things that it sought "to protect the privacy rights of its customers when the government is seeking their data from Amazon, especially when that data may include expressive content protected by the First Amendment. As courts have observed, '[t]he fear of government tracking and censoring one's reading, listening, and viewing choices chills the exercise of First Amendment rights.' " Amazon further argued[xx]:

> Like cell phones, such modern "smart" electronic devices contain a multitude of data that can "reveal much more in combination than any isolated record," allowing those with access to it to reconstruct "[t]he sum of an individual's private life." Riley v. California, 134 S. Ct. 2473, 2489 (2014). The recordings stored by Amazon for a subscriber's Echo device will usually be both (1) the user's speech, in the form of a request for information from Alexa, and (2) a transcript or depiction of the Alexa Voice Service response conveying the information it determines would be most responsive to the user's query. Both types of information are protected speech under the First Amendment.

The case was eventually dropped by the prosecutor, but Amazon's arguments are instructive of a bot service provider's arguments in favor of protections of the speech of customers and of the service provider itself that is embodied in the bot's records.

However, unlike a personal assistant such as Alexa, a Fintech chatbot's records are likely financial records, and there may be weaker arguments for their protections. In *United States v. Miller*[xxi], respondent, who had been charged with various federal offenses, made a pretrial motion to suppress microfilms of checks, deposit slips, and other records relating to his accounts at two banks, which maintained the records pursuant to the Bank Secrecy Act of 1970 (Act). The Supreme Court held that respondent possessed no Fourth Amendment interest in the bank records because among other things, (a) the subpoenaed materials were business records of the banks, not respondent's private papers and (b) there is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications, but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. Here, Fintech bots' records, depending on the facts, may be like bank records that are more like financial transactions and exposed to Fintech company's employees in the ordinary course of business, and thus may have less Fourth and First Amendment protections.

3. Practical and Ethical Considerations

In designing Fintech bots, firms should consider the SEC guidance and FINRA guidance on this subject and put in place proper disclosures of the algorithm used, and the bot should be designed to understand the customer's financial needs. As a practical matter, the bots' records should be stored securely and associated properly with customer accounts for potential audits and discovery by third parties, including law enforcement agencies. While the bot's records may or may not be protected by the Fourth and First Amendment, the bot developer should anticipate

that at some point, those records may be required to be produced, and the Fintech firm should be prepared to have a policy either to produce such records or defend non-disclosure when appropriate. In order to minimize risks that automated transactions entered into by bots are found unenforceable when making commitments on behalf of the Fintech firm or customer, the bot should also clearly obtain consent, including via verbal confirmation code or some other consent mechanism.[xxii]

Questions remain on how courts will treat different type of conversation within a single conversation stream. For example, inside Facebook messenger, the bot queries financial data vs a personal conversation. Another open question as discussed above is how much consent can be delegated to a bot. Think about a comparison shopping switching service for highest interest rate deposit accounts or cheapest electric bills. The electronic agent enters and exits legal agreements on behalf of the client presumably under the instructions of the client. Are those instructions standing instructions? Should bots (or the firms that run them) have a fiduciary duty without dealing in investments?

Beyond the legal requirements, there are ethical considerations, including minimizing any potential bias designed into bots. Machine learning is trained on existing data, which reflects the ways that society and the economy are structured today. But by replicating distributional results, AIs may perpetuate inequities and achieve outcomes that hurt minorities and protected classes. As an example, AIs used in credit underwriting may use thousands of data points, but then overweight items like Zipcode, which can correlate with income levels and ethnicity, prejudicing protected classes. Following ethical norms is not only good policy, it also minimizes legal risk. While we have focused on U.S. law in this article, it should be noted that the EU General Data Protection Regulation (GDPR)[xxiii] including Article 14 and Article 22 will apply to bots that have certain nexus to the EU. Article 22 states that the consumer shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

ENDNOTES:

[i]Fi-Robot: The Rise of Automated "Robo" Investment Advisors, https://news.law.fordham.edu/jcfl/2017/12/29/fi-robot-the-rise-of-automated-robo-investment-advisors/

[ii]#Augmented Finance and Machine Intelligence, https://next.autonomous.com/augmented-finance-machine-intelligence

[iii]*Id* at 43

[iv]*Id*.

[v] https://www.ibm.com/watson/financial-services/

[vi] https://www.finn.ai/

[vii]See 15 U.S.C.A. § 80b-2(11)(A).

[viii]Information for Newly-Registered Investment Advisers, https://www.sec.gov/divisions/investment/advoverview.htm

[ix]Fi-Robot: The Rise of Automated "Robo" Investment Advisors, https://news.law.fordham.edu/jcfl/2017/12/29/fi-robot-the-rise-of-automated-robo-investment-advisors/

[x]SEC Guidance Update, February 2017 | No. 2017-02, https://www.sec.gov/investment/im-guidance-2017-02.pdf

[xi] https://www.finra.org/sites/default/files/digital-investment-advice-report.pdf

[xii]This section is appeared in the co-author's Use of Artificial Intelligence for Smart Contracts

and Blockchains, Fintech Law Report, March/April 2018.

[xiii]Electronic Signatures in Global and National Commerce Act (E-Sign Act), Pub. L. No. 106-229 (2000), https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.

[xiv]National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act (UETA, 1999), http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf.

[xv]The UTEA has not been adopted in New York, Washington, Illinois or Puerto Rico.

[xvi]*State of Arkansas v. Bates*, Case No. 04CR-16-370 (Circuit Court of Benton County, Ark. 2016).

[xvii]Search Warrant, 04CR-16-370-2

[xviii]Motion to Quash Search Warrant, CR-2016-370-2 at 1.

[xix]Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant, CR-2016-370-2 at 2.

[xx]*Id* at 9

[xxi]*U.S. v. Miller*, 1976-1 C.B. 535, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71, 76-1 U.S. Tax Cas. (CCH) P 9380, 37 A.F.T.R.2d 76-1261 (1976).

[xxii]See e.g., Alexa Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740:

1.4 Voice Purchasing. Alexa allows voice purchasing of physical and digital products and services, including subscriptions, from Amazon and other sellers using your default Amazon payment and shipping settings (an "Amazon-Processed Purchase"). You can require a speakable confirmation code, turn off voice purchasing, and see product and order details for Amazon-Processed Purchases in your Alexa App.

[xxiii] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE

MAY/JUNE 2018 REGULATION AND LITIGATION UPDATE

By Duncan Douglass and Samuel Boro

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

REGULATORY DEVELOPMENTS

Mulvaney Seeks Information to Improve CFPB Processes

On January 17, 2018, Mick Mulvaney, the acting Director of the Consumer Financial Protection Bureau ("CFPB"), announced that the agency will be publishing in the *Federal Register* a series of Requests for Information ("RFIs") seeking comment on enforcement, supervision, rulemaking, market monitoring, and education activities. In announcing the upcoming RFIs, Mulvaney said "[m]uch can be done to facilitate greater consumer choice and efficient markets, while vigorously enforcing consumer financial law in a way that guarantees due process."

In the March/April 2018 FinTech Law Report, we discussed the first eight RFIs issued by the CFPB on Civil Investigative Demands; Administrative Proceedings; Enforcement Processes; the CFPB's Supervision Program; External Engagements; Consumer Complaints; Rulemaking Processes; and Adopted Regulations and New Rulemaking Authorities. Since the March/April 2018 FinTech Law Report, the CFPB has released four additional RFIs regarding Inherited Regulations; the CFPB's Guidance and Implementation Support; the CFPB's Financial Education Programs; and the CFPB's Consumer Complaint and Con-

sumer Inquiry Handling Processes (each summarized below). The CFPB intends to issue additional RFIs, including RFIs on Bureau Rules Not Under § 1022(d) Assessment and Consumer Inquiries.

RFI on CFPB's Inherited Regulations

The CFPB issued its ninth RFI, on the CFPB's Inherited Regulations and Inherited Rulemaking Authorities, on March 22, 2018, published in the *Federal Register* on March 26, 2018, seeking comments and information on the regulations and rulemaking authorities that were transferred from other federal agencies to the CFPB by Title X of the Dodd-Frank Act. The RFI does not request feedback regarding the rulemaking process, rules that the CFPB has already issued, or on any implementation guidance, as these topics are subject to separate RFIs. Specifically, this RFI seeks comments and information on whether the CFPB should issue additional regulations and on whether the CFPB should make particular changes to existing inherited regulations. The RFI also notes that the CFPB will consider all comments received under this RFI and the Adopted Regulations RFI together.

Comments must be received by June 25, 2018.

RFI on CFPB's Guidance and Implementation Support

The CFPB issued its tenth RFI, on the CFPB's Guidance and Implementation Support, on March 28, 2018, and published in the *Federal Register* on April 2, 2018, seeking comments and information on the overall effectiveness and accessibility of the CFPB's guidance materials and activities. As defined in the RFI, the CFPB's guidance and implementation support includes interpretive rules and general statements of policy, which have or should have gone through the notice and comment process, as well as non-rule guidance, such as implementation support materials and activities. The CFPB requests that commenters provide specific discussions of positive and negative aspects of the CFPB's guidance materials and activities, and make suggestions regarding potential updates or modifications to these materials. The RFI details a non-exhaustive list of the types of guidance and implementation support that is open to comment (e.g., rule summaries, compliance guides, checklists, institutional and transactional coverage charts, webinars, and other compliance aids).

Comments must be received by July 2, 2018.

RFI on CFPB's Financial Education Programs

The CFPB issued its eleventh RFI, on the CFPB's Financial Education Programs, on April 4, 2018, published in the *Federal Register* on April 9, 2018, seeking comments and information to assess the overall efficiency and effectiveness of its financial education programs. The Consumer Financial Protection Act of 2010 (the "CFPA") requires the CFPB to develop and implement "initiatives intended to educate and empower consumers to make better informed financial decisions."[i] Pursuant to this requirement, the CFPB has developed programs to serve the public, published numerous guides related to different financial topics, and provided financial educators with tools, research, and training on delivering financial education. The RFI seeks comments and information on ways to improve the CFPB's existing programs and delivery mechanisms, as well as ways to better measure and evaluate the effectiveness of the CFPB's education programs, including minimizing dupli-

cation between the CFPB's work and that of other entities and agencies.

Comments must be received by July 9, 2018.

RFI on CFPB's Consumer Complaint and Consumer Inquiry Handling Processes

The CFPB issued its twelfth RFI, on the CFPB's Consumer Complaint and Consumer Inquiry Handling Processes, on April 11, 2018, published in the *Federal Register* on April 17, 2018, seeking comments and information to assist the CFPB in assessing its handling of consumer complaints and consumer inquires. The CFPB defines consumer complaints as "submissions that express dissatisfaction with, or communicate suspicion of wrongful conduct by, an identifiable entity related to a consumer's personal experience with a financial product or service."[ii] The CFPB does not have a published definition of consumer inquiries, so for purposes of the RFI it is defining consumer inquiries as "consumer requests for information—typically proffered by telephone—to its Office of Consumer Response about consumer financial products or services, the status of a complaint, an action taken by the Bureau, and often combinations thereof." In 2017, the CFPB handled more than 320,000 consumer complaints and more than 200,000 consumer inquiries. The RFI seeks specific suggestions for how to improve the consumer complaint and inquiry process, including whether consumers should be required to classify their submissions as either complaints or inquiries prior to submission, and whether there should be a process for companies to reclassify consumers' submissions.

Comments must be received by July 16, 2018.

CFPB Issues Semi-Annual Report to Congress

On April 4, 2018, the CFPB issued its twelfth Semi-Annual Report covering the period from April 1, 2017 through September 1, 2017. The majority of the Semi-Annual Report provides a detailed assessment of the CFPB's rulemaking, supervision, and enforcement actions over the prior year.

Acting Director Mulvaney appeared before the House Financial Services Committee on April 11, 2018 to take questions from law makers regarding the Semi-Annual Report.

The Semi-Annual Report opens with a letter from Mulvaney that tells Congress that "the Bureau is far too powerful, and with precious little oversight of its activities." Specifically, Mulvaney notes in his letter that the Director serves "as a one-man legislature empowered to write rules to bind parties in new ways; as an executive officer subject to limited control by the President; and as an appellate judge presiding over the Bureau's in-house court-like adjudications." He argues that the very statutory structure of the CFPB creates "an agency primed to ignore due process and abandon the rule of law in favor of bureaucratic fiat and administrative absolutism." Accordingly, Mulvaney requests four changes to the legislation creating the CFPB:

(1) Fund the CFPB through Congressional appropriations;

(2) Require legislative approval of major CFPB rules;

(3) Ensure that the Director answers to the President in the exercise of executive authority; and

(4) Create an independent Inspector General for the CFPB.

The Semi-Annual Report also provides a list of upcoming proposed rules:

(1) A rulemaking to reconsider the CFPB's Payday Lending Final Rule;

(2) A rule amending Regulation CC issued jointly with the Federal Reserve;

(3) A rule addressing creditor disclosures to borrowers and debt collectors' communications practices under the Fair Debt Collection Practices Act; and

(4) A rulemaking to reconsider aspects of the CFPB's 2015 Home Mortgage Disclosure Act rule.

Finally, the Semi-Annual Report provides a list of upcoming final rules:

(1) Amendments to Regulation P, which implements the Gramm-Leach-Bliley Act, concerning annual notice requirements;

(2) Amendments relating to disclosure of CFPB records and information procedures under the Freedom of Information Act, including the protection and disclosure of confidential information that the CFPB obtains in connection with the exercise of its authorities; and

(3) Amendments to the Federal Mortgage Disclosure Requirements under the Truth in Lending Act ("TILA") and Regulation Z related to the use of closing disclosures to determine good faith disclosure of estimated closing cost.

Federal Reserve Requests Comment on Amendments to Regulation J

On March 6, 2018, the Board of Governors of the Federal Reserve System (the "Board") announced a proposed rule amending Regulation J, Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire (12 C.F.R. Part 210) (the "Regulation J Proposed Rule"), seeking comment on proposed amendments to (i) clarify and simplify certain provisions of Subpart A (Collection of Checks and other Items by Federal Reserve Banks); (ii) remove obsolete provisions; (iii) align the rights and obligations of sending banks, paying banks, and Federal Reserve Banks ("Reserve Banks") with the Board's May 2017 final rule amending Regulation CC, Availability of Funds and Collection of Checks (12 C.F.R. Part 229) ("Regulation CC Final Rule"), to reflect the current electronic check collection and return environment; and (iv) amend Subpart B (Funds Transfers Through Fedwire) to clarify terms used in financial messaging standards. If finalized, the Regulation J Proposed Rule would become effective July 1, 2018. Comments must be submitted within 60 days of publication in the *Federal Register*. As of the date of this memorandum, the Regulation J Proposed Rule has not been published in the *Federal Register*.

In May 2017, the Board issued the Regulation CC Final Rule, which reflected the "virtually all-electronic check collection and return environment" by, among other things, adding defined terms for "electronic check" and "electronic returned checks," and modifying and creating warranties and indemnifications.[iii] The Regulation J Proposed Rule is written to align Regulation J with the distinction between checks and

electronically-created items ("ECIs") in Regulation CC. Specifically, the Regulation J Proposed Rule amends the definitions of "check" and "returned check," deletes Regulation J's current definition of "electronic item," and amends the definition of "item," in order to make Regulation J encompass ECIs so Reserve Banks are permitted to accept ECIs under the regulations. The definition of "check" in Regulation J would be amended to have the same meaning as the terms "check" and "electronic check" in Regulation CC.[iv] The term "item" would be amended to include the term "check" with its new definition referencing the term in Regulation CC.[v]

The Regulation J Proposed Rule would also allow a Reserve Bank to require a sender to warrant that such sender will only send those "items" and "noncash items" that the Reserve Bank has agreed to accept, and to indemnify the Reserve Bank for any loss resulting from the sender's failure to do so.[vi] The Board notes that this change will "help shift liability to parties better positioned to know whether an item is electronically created and to prevent the item from entering the check-collection system."[vii] The Regulation J Proposed Rule would not, however, prevent parties from exchanging ECIs by agreement using direct exchange relationships or other methods not involving Reserve Banks. In short, Regulation J's sender warranties would align with the warranties specified in Regulation CC.[viii] The Board requests comment on whether it should consider amending Regulation J in a future rulemaking to permit Reserve Banks to accept ECIs.

The Regulation J Proposed Rule also proposes to revise some of Regulation J's settlement provisions to remove references to cash and certain other forms of settlement, and instead states that the Reserve Banks may settle by debit to an account on the Reserve Bank's books, or another acceptable form of settlement. The Board requests comment on possible implications that the proposed changes may have on financial institutions.

Finally, the Regulation J Proposed Rule would create a new subsection to clarify that financial messaging standards, like ISO 20022, including the components of the financial messaging, the elements, technical documentation, tags, and terminology used to implement those standards, do not confer legal status or responsibilities. Instead the Regulation J Proposed Rule states that Regulation J, Article 4A of the U.C.C., and the Reserve Banks' operating circulars govern the rights and obligations of the parties to the Fedwire Funds Service.[ix]

You can read the Regulation J Proposed Rule here:

https://www.federalreserve.gov/newsevents/pressreleases/bcreg20180306a.htm

FinCEN Issues Updated FAQs Regarding its Customer Due Diligence Rule

On April 3, 2018, the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the U.S. Department of the Treasury, issued supplemental FAQs regarding customer due diligence requirements for certain financial institutions (the "Customer Due Diligence Rule").[x] FinCEN issued the Customer Due Diligence Rule on May 11, 2016[xi], and first issued FAQs regarding the rule on July 19, 2016.[xii]

The Customer Due Diligence Rule applies to "covered financial institutions," which include insured banks, commercial banks, agencies or

branches of a foreign bank in the United States, federally-insured credit unions, savings associations, corporations acting under section 25A of the Federal Reserve Act, trust banks or trust companies that are federally regulated and are subject to an anti-money laundering program requirement, certain securities brokers or dealers, and certain futures commission merchants or introducing brokers.[xiii] Accordingly, the Customer Due Diligence Rule does not apply to nonbank money services businesses that do not meet the definition of "covered financial institution."

The Customer Due Diligence Rule applies to "those financial institutions already covered by [Customer Identification Program ("CIP")] requirements."[xiv] FinCEN explained, however, that it "believe[s] that extending CDD requirements in the future to [institutions not subject to CIP], and potentially other types of financial institutions, may ultimately promote a more consistent, reliable, and effective AML regulatory structure across the financial system."[xv]

Covered financial institutions are required "to establish and maintain written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers and to include such procedures in their anti-money laundering compliance program required under 31 U.S.C.A. 5318(h) and its implementing regulations."

The updated FAQs include 37 FAQs and responses that clarify FinCEN's expectations and certain other implementation issues for affected financial institutions. Some of the important issues addressed in the FAQs include the following topics:

- *Defining "New Account"* - FAQ #11 clarifies that a "new account" is defined to mean "each account *opened . . . by a legal entity customer*" (emphasis in FAQs). FAQ #11 explains that accounts created by the financial institution for its own administrative or operational purposes and not at the customer's request are not new accounts for purposes of the Customer Due Diligence Rule. This interpretation is limited, however, to accounts "created solely to accommodate the business of an *existing* legal entity customer that has previously identified its beneficial ownership" (emphasis in FAQs). FAQ #12 states that a "new account" is created when "the bank establishes another formal banking relationship." Accordingly, certain loan renewals or CD rollovers, for example, are "not generally treated as new accounts by the industry and the risk of money laundering is very low, if at the time the customer certifies its beneficial ownership information, it also agrees to notify the financial institution of any change in such information." The original beneficial ownership information collected when the loan or CD is created would therefore suffice for as long as the loan or CD is outstanding.
- *Existing Customers* - FAQ #7 explains that if an individual is identified as a beneficial owner, but that same individual is an existing customer of the financial institution and is subject to the financial institution's CIP procedures, then the financial institution may rely on information already in its possession to fulfill identification and verification requirements, provided that the existing information is up-to-date and accurate, and the legal entity customer's representa-

tive certifies or confirms the accuracy of the information.

- *Methods of Verifying Beneficial Ownership Information* - FAQ #4 explains that a financial institution must verify the identity of each beneficial owner according to risk-based procedures that contain, at a minimum, the same elements the financial institution is required to use to verify the identity of individual customers under applicable CIP requirements. The FAQ makes a distinction between a financial institution's CIP procedures and its beneficial ownership procedures, noting that the procedures must contain the same elements, but need not be identical.

- *Updating Beneficial Ownership Information* - Numerous FAQs address how and when beneficial ownership information must be or could be updated. FAQ #13 and FAQ #14 both confirm (or, "support the view") that the need to update beneficial ownership information generally depends on whether there is a triggering event or knowledge on the part of the financial institution of a change in the information. FAQ #16 explains that a covered financial institution may need to physically obtain and recertify beneficial ownership depending on the change. The determining factor generally depends on the materiality of the change. FAQ #16 notes that updating an address would likely not require full recertification, whereas a new beneficial owner would require all information to be collected, certified, and verified.

- *Private Label Retail Credit Accounts Point-of-Sale Exemption* - FAQ #29 clarifies the exemption from the requirements for a covered financial institution that "opens an account for a legal entity customer that is: [a]t the point-of-sale to provide credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of $50,000." It states that the point-of-sale exemption is "provided for retail credit accounts opened to facilitate purchases made at the retailer because of the very low risk posed by opening such accounts at the brick and mortar store." (emphasis added).

FTC Issues Informal P2P Payments Guidance

On February 27, 2018, the Federal Trade Commission ("FTC") published a blog post with tips for consumers on how to use peer-to-peer ("P2P") payment systems and applications. The blog post provides a brief summary of what P2P payment systems do, and warns consumers about how money moves into and out of a P2P system or application and the potential for scams or exposure of personal information when using such systems. With regard to the transfer of funds, the blog post warns consumers that transfers from a P2P system to the consumer's bank account may take a few days or longer if they are flagged for additional review. The blog post also warns that scammers may encourage the use of P2P systems for the purchase of an item like a concert ticket, and that sellers should ensure that they have received the purchase price in their accounts before sending any goods to purchasers. Finally, the blog post warns that P2P payment systems frequently access a consumer's bank account information, and may also share a consumer's

transaction information on social media. It encourages consumers to enable additional security measures, like multi-factor authentication, and to review social media permissions or settings to maintain privacy.

The FTC published this blog post in conjunction with its announcement of its settlement with P2P payment system and app, Venmo. The FTC-Venmo settlement is discussed below in the Litigation and Enforcement Developments section of this memorandum.

GAO Issues FinTech Marketplace Report

On March 22, 2018, the Government Accountability Office ("GAO") issued a report detailing steps regulators could take to protect consumers and aid regulatory oversight of the FinTech marketplace. The report notes that FinTech products generally benefit consumers through convenience and lower costs. However, the risks associated with FinTech products "may not always be sufficiently addressed by existing laws and regulations."[xvi] Identified risks include data security and privacy concerns that could affect overall financial stability as the FinTech company grows. The report also notes that FinTech companies are complying with varying federal and state requirements that are "costly and time-consuming" to the companies. Further, overlapping regulatory oversight leaves room for significant collaboration between agencies. The report provides suggestions for such collaboration. Finally, the report evaluates the feasibility of adopting regulatory approaches similar to those taken by regulators outside the U.S. with regard to FinTech companies, with emphasis on regulatory sandbox approaches. Other federal regulators supported the GAO's findings in comment letters, including the CFPB, the Commodity Futures Trading Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Board, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.

NYDFS Updates Cybersecurity Regulation FAQs

On February 21, 2018, the New York Department of Financial Services ("NYDFS") updated its FAQs for its cybersecurity regulation (the "Cybersecurity Final Rule") (23 NYCRR Part 500). The NYDFS had previously updated its FAQs for the Cybersecurity Final Rule in December 2017. The Cybersecurity Final Rule applies to a "covered entity," which is defined as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law [of New York]."[xvii] The Cybersecurity Final Rule requires, in relevant part, that a covered entity maintain a cybersecurity program, implement and maintain a written cybersecurity policy, implement a third-party service provider security policy, and establish an incident response plan.[xviii]

In particular, the updated FAQs provide the following guidance:

- Due to the increase in cybersecurity risks that financial institutions face, the NYDFS is "strongly encourag[ing] all financial institutions, including exempt Mortgage Servicers, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500;"
- Not-for-profit mortgage brokers are "cov-

ered entities" under the Cybersecurity Final Rule (see FAQ #2);

- Covered entities, when acquiring or merging with a new company, must conduct a factual analysis of how the Cybersecurity Final Rule applies to the transaction. The NYDFS emphasizes that during new acquisitions, covered entities "need to have a serious due diligence process and cybersecurity should be a priority" (see FAQ #3); and
- Health Maintenance Organizations and continuing care retirement communities are "covered entities" under the Cybersecurity Final Rule (see FAQ #4).

NYDFS Issues Virtual Currency Guidance

On February 7, 2018, the NYDFS issued guidance for virtual currency businesses licensed under 23 NYCRR Part 200 or chartered as limited purpose trust companies under the New York Banking Law.[xix] The guidance is issued in response to the risk of fraud in the cryptocurrency market that the NYDFS sees as a growing concern.[xx]

The guidance directs that virtual currency businesses implement a written policy that (i) identifies and assesses the full range of fraud-related and similar risk areas, including, as applicable, market manipulation; (ii) provides effective procedures and controls to protect against identified risks; (iii) allocates responsibility for monitoring risks; and (iv) provides for the effective investigation of suspected or actual fraud and other wrongdoing, including, as applicable, market manipulation.

In the event that a virtual currency business discovers any wrongdoing, it must submit to the NYDFS a report with all pertinent details about the wrongdoing. In addition, virtual currency businesses must submit to the NYDFS, as soon as practicable, a further report or reports of any material developments related to the original report, along with a statement of actions taken or proposed to be taken in response to these developments, and a statement of changes in the virtual currency business' operations to avoid repetition of similar events.

Department of the Treasury Publishes Letter Regarding Its Oversight and Enforcement of Virtual Currencies and ICOs

On February 13, 2018, the U.S. Department of the Treasury published a letter responding to Senator Ron Wyden's (D-Or.) request for information regarding FinCEN's oversight and enforcement capabilities over virtual currency financial activities. The letter highlights FinCEN's work engaging with other regulators on issues related to virtual currency and initial coin offerings ("ICOs"). In addition to the summary of FinCEN's work in this space, the letter states that existing regulations and interpretations provide that a company that "sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency" such as other virtual currency, is a money transmitter, and must comply with FinCEN's anti-money laundering regulations, including the Bank Secrecy Act and know-your-customer guidelines. Further, the letter states that an exchange that "sells ICO coins or tokens, or exchanges them for other virtual currency, fiat currency, or other value that substi-

tutes for currency," would also typically be a money transmitter.

Prior FinCEN guidance indicates that a "user" of convertible virtual currency[xxi] is not a money transmitter, and that a person may "mine," "create," or "manufacture" a virtual currency without being a money transmitter.[xxii] That guidance also states that an "exchanger" or "administrator" of convertible virtual currency is a money transmitter unless a limitation to or exemption from the definition of "money transmitter" applies to the person.[xxiii] FinCEN's letter does not define what ICO coins or tokens are, nor does it attempt to provide a comprehensive analysis of what actions will make a person a money transmitter. Instead, the letter explains that the anti-money laundering obligations for participants in ICOs "will depend on the nature of the financial activity involved in any particular ICO," based on "the facts and circumstances of each case."

LITIGATION DEVELOPMENTS

PayPal Settles with FTC Regarding Venmo's GLBA Failures

On February 27, 2018, the FTC reached a settlement with PayPal, Inc. ("PayPal") over allegations that PayPal's mobile P2P payment service app Venmo misled users about aspects of user accounts, including the availability of their balances and the privacy of their transactions. PayPal is not required to pay a fine, but will be required to modify its policies, procedures, and disclosures, and be subject to third-party audits of Venmo's privacy and data security practices for 10 years. The allegations in the complaint include violations of the FTC Act when Venmo (i) misrepresented the availability of users' funds; and (ii) misrepresented and failed to properly disclose how a user could adjust their privacy settings. In addition, the complaint alleged that Venmo failed to provide clear and conspicuous initial privacy notices and failed to implement appropriate safeguards in violation of the GLBA.

Venmo is a mobile P2P application that enables consumers to connect their bank account or credit or debit card to the user's Venmo account in order to send and receive money between Venmo users. Each Venmo user may also transfer his or her funds in the user's Venmo account to the user's linked bank account. When a Venmo user sends money through Venmo to another user, the recipient is notified within seconds of the transfer. In many instances, the notifications have informed the recipient that they have been paid and can transfer the money to an external bank account.

Funds Availability Representations

According to the compliant, Venmo represented that a consumer can transfer funds to their bank account within a specific time frame, often "overnight," or "in as little as one business day," which led Venmo users to believe that when they receive a payment notification, the funds would be available to transfer to an external bank account.[xxiv] In numerous instances, consumers were unable to transfer funds as quickly and easily as Venmo's notifications led them to believe. The complaint asserts that Venmo often waited until a consumer attempted to transfer funds to an external bank account before reviewing the P2P transaction for fraud, insufficient funds, or other problems. Occasionally, Venmo required users to provide documentation or other information as part of the review, and sometimes the users' accounts were frozen during the review. If Venmo reversed a transaction, it removed the

funds from that transaction from the user's Venmo balance.

Venmo received thousands of consumer complaints about delays or loss of funds, and many consumers reported significant financial hardships as a result of these delays and losses, including the inability to pay rent or other bills with funds they expected to be able to retrieve from their Venmo accounts. In the settlement order, Venmo is directed that when it makes a representation about the availability of funds to be transferred or withdrawn to a bank account it "(1) must disclose, clearly and conspicuously, and in close proximity to such representation (a) that the transaction is subject to review and (b) the fact, if true, that funds could be frozen or removed as a result of transaction reviews performed during the bank transfer or withdrawal process, and (2) the representation must not be otherwise misleading."[xxv]

Privacy Representations

The complaint also alleged that Venmo misrepresented how users could protect their privacy when conducting transactions through Venmo. By default, all P2P transactions on Venmo were displayed on Venmo's social news feed. The news feed displayed the names of the payer and recipient, the date of the transaction, and a message written by the user that initiated the transaction. These pieces of information would be displayed to anyone using Venmo's app. In addition, each Venmo user has a profile page on Venmo's website that listed the user's transactions, and the user's five most recent public Venmo transactions were visible to anyone who views that user's profile page, even if that person does not have a Venmo account.[xxvi] A user could restrict the visibility of his or her transactions through privacy settings in a "Settings" menu or by adjusting the settings for an individual transaction. If a consumer wished to restrict the visibility of all future transactions, the user was required to change two similarly labeled settings that (1) limit the default audience for future transactions; and (2) determine who can share transactions involving the user. If the user did not change both privacy settings, then a transaction could still be displayed publicly if the other Venmo user involved in the P2P transaction had not changed his or her default settings or marked an individual transaction public. The complaint asserts that Venmo had not informed users that another user could override a user's default settings if both privacy settings were not adjusted correctly. Even Venmo's Privacy FAQs failed to accurately describe the interplay between the two privacy settings. These results, the complaint states, "are directly contrary to the expectations of a reasonable consumer."[xxvii]

To resolve the identified issues with Venmo's privacy practices, the settlement order directs that Venmo "must clearly and conspicuously disclose to each User, through the Payment and Social Networking Service, and separate and apart from any "privacy policy," "terms of use," "blog," "helpful information" page, or similar document: (1) how the User's transaction information will be shared with other Users; and (2) how the User can use privacy settings to limit or restrict the visibility or sharing of the User's transaction information on the Payment and Social Networking Service."[xxviii]

GLBA Violations

The complaint alleged that, as a covered entity, Venmo failed to comply with the GLBA's Safeguards and Privacy Rules, and Regulation P. Both

the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice that is clear and conspicuous and accurately reflects the financial institution's privacy policies and practices. The notices must be provided so that each consumer can reasonably be expected to receive notice. The Safeguards Rule requires that financial institutions protect the security, confidentiality, and integrity of customer information through comprehensive written information security programs that contain reasonable safeguards for the information.

The complaint alleged that Venmo's initial privacy notice was not clear and conspicuous, in violation of the Privacy Rule and Regulation P, because the link to the privacy policy was only shown in gray text on a light gray background on a screen during the sign up process.[xxix] Venmo's privacy policy was also inaccurate because Venmo represented in the policy that it shared a user's personal information with the user's "social web" if the user's transactions are designated as "public" or "friends-only payments," but in fact Venmo shared the user's information with *everyone* on the internet by default, and not just a user's social web.[xxx] Venmo also allegedly failed to deliver the initial privacy notice so that each user could reasonably be expected to receive actual notice. Venmo did not require customers to acknowledge receipt of an initial privacy notice, which is required for consumers to obtain a financial product or service.[xxxi]

Venmo also allegedly violated the Safeguards Rule by (i) failing to have a written information security program through at least August 2014; (ii) failing to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information through at least September 2014; and (iii) failing to implement basic safeguards for consumer information until approximately March 2015, including failing to provide security notifications to consumers and failing to maintain adequate customer support to timely investigate and respond to users' reports about account compromises or unauthorized transactions.[xxxii]

National Bank Act Held to Not Preempt California Law on Mortgage Escrow Accounts

On March 2, 2018, a three-judge panel for the U.S. Court of Appeals for the Ninth Circuit (the "Ninth Circuit") unanimously held that a class action suit against Bank of America, N.A. ("Bank of America") could proceed because the National Bank Act does not preempt a California state consumer protection law that requires a bank to pay interest on mortgage escrow accounts. The Ninth Circuit held that the California law does not interfere with the bank's exercise of its banking powers under federal law.

The plaintiff filed suit on behalf of a proposed class of Bank of America customers, alleging that Bank of America violated 15 U.S.C.A. § 1639d(g)(3), which amends TILA, California's state mortgage escrow interest law (Cal. Civil Code § 2954.8(a))[xxxiii], and the "unlawful" prong of the California Unfair Competition Law (the "UCL"). The plaintiff also brought a breach of contract claim. Bank of America moved to dismiss on the ground that California's state escrow interest law is preempted by the National Bank Act.

The plaintiff's mortgage was held by Bank of America. The mortgage agreement stated that the

plaintiff's mortgage "shall be governed by federal law and the law of the jurisdiction in which the Property is located."[xxxiv] The mortgage agreement further stated that Bank of America was required to pay interest on escrow funds if required by federal law or by state law that is not preempted. Bank of America acknowledged that it did not pay interest on the plaintiff's mortgage escrow account even though other national banks in California abided by the state law. The Ninth Circuit conducted its preemption analysis in light of provisions of the Truth in Lending Act, as amended by the Dodd-Frank Act, and the Dodd-Frank Act's modification of National Bank Act preemption standards.

In relevant part, the Truth in Lending Act provides that "If prescribed by applicable State or Federal law, each creditor shall pay interest to the consumer on the amount held in any impound, trust, or escrow account that is subject to this section in the manner as prescribed by that applicable State or Federal law."[xxxv] Bank of America argued that the National Bank Act preempted California's state mortgage escrow interest law because state laws like California's "prevent[] or significantly interfere[] with the exercise by a national bank of its powers."[xxxvi] A preempted law, Bank of America argues, cannot be an "applicable" law as required by section 1639d(g)(3) of the Truth in Lending Act. The plaintiff argued, however, that the Truth in Lending Act's plain language makes clear that Congress perceived no conflict between state laws such as California's state escrow interest law and the powers of national banks.[xxxvii]

The Ninth Circuit engaged in a preemption analysis. It first noted that consumer protection laws are generally a purview of the states, so that "compelling evidence of an intention to preempt is required."[xxxviii] Accordingly, the Ninth Circuit stated that Bank of America must "affirmatively demonstrate" that Congress intended to preempt state escrow interest law.[xxxix] The Ninth Circuit then explained that, as provided in the Dodd-Frank Act, the applicable preemption standard is found in *Barnett Bank of Marion County, N.A. v. Nelson*,[xl] which held that states are not "deprive[d] . . . of the power to regulate national banks, where . . . doing so does not *prevent or significantly interfere* with the national bank's exercise of its powers."[xli]

Under the *Barnett Bank* standard, the Ninth Circuit determined that the California law is not preempted because it does not prevent or significantly interfere with Bank of America's exercise of its powers. Importantly, the Ninth Circuit noted, Congress expressed its view that laws like the California escrow interest law would not necessarily prevent or significantly interfere with a national bank's operations, when it stated in section 1639d(g)(3) of the Truth in Lending Act that banks may be required to pay interest on mortgage escrow accounts "if prescribed by applicable State . . . law."[xlii]

On April 13, 2018, Bank of America filed a petition for rehearing *en banc*, which was denied on May 16, 2018.

The case before the Ninth Circuit was: *Lusnak v. Bank of America, N.A.*, No. 14-56755

The Bancorp Bank Faces FDIC Order for Prepaid Card Fees

On March 7, 2018, the Federal Deposit Insurance Corporation ("FDIC") issued an order to The Bancorp Bank ("Bancorp") requiring restitu-

tion and the payment of civil money penalties.[xliii] The order requires Bancorp to establish a $1.3 million restitution fund for eligible customers and to pay $2 million in civil money penalties. The order further requires that Bancorp retain all records pertaining to the restitution required by the order for a period of seven years, and to furnish the FDIC with written quarterly progress reports. The order stemmed from the FDIC's findings that Bancorp's prepaid card program violated Section 5 of the FTC Act (15 U.S.C.A. § 45(a)(1)); the Electronic Fund Transfer Act (15 U.S.C.A. § 1693 et seq.) and Regulation E (12 C.F.R. Part 1005); the Truth in Savings Act (12 U.S.C.A. § 3201 et seq.) and Regulation DD (12 C.F.R. Part 1030); and the Electronic Signatures in Global and National Commerce Act (15 U.S.C.A. § 7001 et seq.).

The order does not provide details about the violations except to note that the FTC Act violations resulted from Bancorp improperly disclosing and assessing transaction fees for point-of-sale signature-based transactions without a personal identification number ("PINless transactions") and certain other general purpose reloadable debit cards. The transaction fees were assessed by Bancorp's third party payment processor for PINless transactions, and were greater than Bancorp had disclosed to customers for such transactions.[xliv]

Amex "No-Steering" Antitrust Case Proceeds to Oral Argument at the Supreme Court

On February 26, 2018, the U.S. Supreme Court heard oral argument in the antitrust case against American Express Co. ("Amex") regarding its nondiscrimination rules. Amex's nondiscrimination rules (also known as anti-steering or no-steering rules), prohibit merchants from "(1) offering customers any discounts or nonmonetary incentives to use cards that are less costly for merchants to accept, (2) expressing preferences for any card, or (3) disclosing information about the costs to merchants of different cards."[xlv] The U.S. Court of Appeals for the Second Circuit ("Second Circuit") reversed the district court's decision, holding that "[t]he District Court erred here in focusing entirely on the interests of merchants while discounting the interests of cardholders," and explained that the plaintiffs failed to "prove net harm to Amex consumers as a whole—that is, both cardholders and merchants—by showing that Amex's nondiscriminatory provisions have reduced the quality or quantity of credit-card purchases."[xlvi] The Second Circuit noted additional flaws in the district court's reasoning, including its consideration of what constituted a "relevant market,"[xlvii] its interpretation of the phrase "market power,"[xlviii] and its assessment of actual adverse effect on competition.[xlix]

Of particular interest to the antitrust bar, the Supreme Court's decision in this case is likely to affect how courts conduct a "rule of reason" analysis with regard to a two-sided market like the credit card industry, in a situation where a company like Amex provides its services to both sides of the market, e.g., merchants and cardholders. Under antitrust law the "rule of reason" requires a plaintiff to show that a defendant with market power has engaged in anticompetitive conduct.

The briefs before the Supreme Court debate the proper definition of "market power." In its brief to the Supreme Court, Amex argued that it does not have market power because its market share is limited to 10% of the credit cards in

circulation, and its credit cards are accepted by roughly one-third fewer merchants than its competitors. Amex also argued that the nondiscrimination provisions constitute vertical agreements between operators throughout the supply chain, and that vertical restraints are presumptively procompetitive, unless they are employed by a company with a large market share.[l] The states, in reply, argue that Amex misconstrues how the courts should view market power. The states argue that market power can be proven directly or indirectly. Under the indirect method, the courts may estimate a defendant's market power by "considering its share of a properly defined market."[li] Under the direct method, however, " 'proof of actual detrimental effects, such as a reduction of output, can obviate' the need for the indirect inquiry."[lii] Accordingly, the states argue that the "indirect method estimates whether a party *might* affect industry prices; the direct method shows that the party *has* done so."[liii]

In oral argument, the justices asked hard questions of both sides. Justice Gorsuch led the questioning, asking counsel for the states whether there was any evidence of restricted output in the case because "that's normally what the antitrust laws care about . . . deadweight loss." He went on to state that the states had no proof that "on a net basis, consumers pay more." Justice Sotomayor quickly came to the defense of the states when counsel did not sufficiently counter Gorsuch's questions. Sotomayor asked, and counsel agreed, that Amex's restriction meant that a merchant could not offer a discount for using another card brand.

Gorsuch also placed pointed questions to counsel for the United States, who was appearing in support of Amex, asking counsel to weigh in on whether "judicial errors are a lot harder to correct than an occasional monopoly where you can hope and assume that the market will eventually correct it." He asked this in an effort to force counsel to state why the Court should adopt Amex's position and thereby establish judicial precedent in this area. Justice Kennedy and Justice Kagan then pushed counsel to walk through the United States' method of analyzing the relevant market because, as Kennedy suggested, it appeared that the United States thought the Court should ignore the cardholders side of the two-sided market when considering if the plaintiff has established an anticompetitive effect.

Sotomayor led the questioning of counsel for Amex, asking counsel to tell her why Amex's anti-steering provisions do not remove competition. Her question included an example of a merchant offering a consumer a discount not to use her Amex card for a transaction in exchange for a discount, which provides the consumer with the choice of whether to earn rewards points by using her Amex card or choosing to use a different method of payment and getting a discount at the register. When counsel redirected the thrust of the question with his answer, arguing that the loss of rewards points is a price increase to the consumer as well, Sotomayor stated that Amex is making the consumer's choice for her, and her choice is "what price competition is all about." Many of the justices then posed numerous hypotheticals to Amex counsel in an effort to have counsel explain why anti-steering provisions were not anticompetitive, and to show why Amex counsel argued that the anti-steering provisions were actually pro-competitive. Questions in this vein came from both liberal and conservative justices, but it is not clear after question-

ing where the justices ultimately stand on the issue in this case.

The case before the U.S. Supreme Court is: *Ohio v. American Express Co.,* No. 16-1454

Trade Groups Sue CFPB Over Payday Lending Final Rule

On April 9, 2018, two trade groups, the Community Financial Services Association of America, Ltd. and the Consumer Service Alliance of Texas, filed a lawsuit against the CFPB to challenge the Payday Lending Final Rule. The lawsuit seeks an order that the Payday Lending Final Rule is unlawful. The case is before the U.S. District Court for the Western District of Texas.

The complaint alleges a number of reasons why the Payday Lending Final Rule is unlawful, including:

- The CFPB's structure is unconstitutional;
- The CFPA unconstitutionally delegates legislative power to the CFPB where it grants the CFPB power to prescribe rules regarding unfair, deceptive, or abusive acts or practices;
- The Payday Lending Final Rule is an action in excess of the CFPB's statutory authority because (1) the rule's identification of unfair and abusive lending practices conflicts with the CFPB's authority to declare an act or practice unfair or abusive under the CFPA; (2) the rule violates the CFPA's prohibition on the CFPB establishing a usury limit because the rule "determines the legal status of certain covered loans based solely on interest rates;" and (3) the CFPB does not have the authority to impose ability-to-repay requirements on the loans covered by the rule;
- The Payday Lending Final Rule is arbitrary and capricious in violation of the Administrative Procedure Act (the "APA") because the CFPB's determinations that the rule is unfair and abusive are unsupported by substantial evidence and reflect a clear error in judgment;
- The CFPB's cost-benefit analysis of the Payday Lending Final Rule does not satisfy the CFPB's requirements with regard to such an analysis; and
- The CFPB failed to observe certain procedural requirements for promulgation of the Payday Lending Final Rule, including (1) violations of the APA's notice and comment process by failing to consider evidence that differs from the CFPB's predetermined decision that payday lending is harmful; (2) the CFPB "reduced the elaborate rulemaking process to little more than a sham" by allowing outside groups opposed to the payday lending industry to control the rulemaking; (3) violations of the Small Business Regulatory Enforcement Fairness Act when the CFPB failed to adequately consider the rule's effect on small businesses; and (4) the CFPB failed to give adequate consideration to consumer comments on the proposed rule if the comments opposed the proposed rule.

The case before the U.S. District Court for the Western District of Texas is: Community Financial Services Association of America, Ltd., and Consumer Service Alliance of Texas v. Consumer

Financial Protection Bureau, Case No. 1:18-cv-00295.

Chase Bank Faces Suit Over Cryptocurrency Fees

On April 10, 2018, a class action complaint was filed against Chase Bank USA, N.A. ("Chase") alleging that Chase began considering cryptocurrency purchases made with a credit card to be cash advances instead of ordinary purchase transactions, resulting in consumers incurring fees and higher interest charges without warning. According to the complaint, the class members purchased cryptocurrencies from Coinbase.com, a cryptocurrency exchange, using personal credit cards, and those purchases were treated like ordinary purchase transactions until late January 2018 when Chase began considering cryptocurrency purchases to be cash advances without notice to consumers. The change in Chase's policy is alleged to be a violation of TILA and Regulation Z. The complaint seeks a refund of all cash advance charges and interest levied against the consumers in connection with cryptocurrency purchases. The case is before the U.S. District Court for the Southern District of New York.

The plaintiff's allegations related to TILA and Regulation Z state that credit card issuers are required to "provide a written notice of any significant change, as determined by rule of the Bureau, in the terms . . . of the cardholder agreement between the creditor and obligor, not later than 45 days prior to the effective date of the change."[liv] The complaint further alleges that Regulation Z states that changes in cash advance fees are considered a "significant change in account terms" under the regulation. The complaint also states that, in the alternative, even if the change is not a "significant change in account terms," the creditor is required to either provide the 45-day notice or provide notice prior to the consumer agreeing to or becoming obligated to pay the charge.

The case before the U.S. District Court for the Southern District of New York is: *Tucker v. Chase Bank USA, N.A.*, Case No. 1:18-cv-03155-ER.

ENDNOTES:

[i]12 U.S.C.A. § 5493(d)(1).

[ii]*See* CFPB, Consumer Response Annual Report (Mar. 2012).

[iii]Federal Reserve System, Proposed Rule, Docket No. R-1599, p. 3 (Mar. 6, 2018), available at https://www.federalreserve.gov/newsevents/pressreleases/bcreg20180306a.htm.

[iv]*See* Regulation J Proposed Rule, 12 C.F.R. § 210.2(h).

[v]*See* Regulation J Proposed Rule, 12 C.F.R. § 210.2(i).

[vi]*Id.* at 5; *see* Regulation J Proposed Rule, 12 C.F.R. § 210.5(a).

[vii]*Id.*

[viii]The Regulation J Proposed Rule makes conforming changes to numerous subsections of Regulation J to align its requirements with the changes made to Regulation CC in the Regulation CC Final Rule.

[ix]Federal Reserve System, Proposed Rule, Docket No. R-1599, p. 14 (Mar. 6, 2018).

[x]FIN-2018-G001, Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (Apr. 3, 2018).

[xi]81 FR 29398 (May 11, 2016).

[xii]FIN-2016-G003, Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (July 19, 2016).

[xiii]*See* 31 C.F.R. § 1010.230(f) (citing *id.* at

§ 1010.605(e)(1)).

[xiv]81 Fed. Reg. at 29417.

[xv]*Id.*

[xvi]GAO-18-254, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight, (March 2018).

[xvii]23 NYCRR § 500.01(c).

[xviii]*See* 23 NYCRR § 500.02, § 500.03, § 500.11, and § 500.16.

[xix]NYDFS has approved six firms for virtual currency charters or licenses. They are bitFlyer USA, Coinbase Inc., XRP II, Circle Internet Financial, Gemini Trust Company, and itBit Trust Company. NYDFS Press Release, DFS Takes Action to Deter Fraud and Manipulation in Virtual Currency Markets (Feb. 7, 2018), available at http://www.dfs.ny.gov/about/press/pr1802071.htm.

[xx]*Id.*

[xxi]*See* FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013) (explaining that the definition of money transmitter "does not differentiate between real currencies and convertible virtual currencies," but rather considers whether a person is "[a]ccepting and transmitting anything of value that substitutes for currency" for purposes of determining whether a person is a money transmitter).

[xxii]*See* FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013) (defining a "user" as a person that obtains virtual currency to purchase goods or services); FIN-2014-R001, Application of FinCEN's Regulations to Virtual Currency Mining Operations (Jan. 30, 2014) (stating that virtual currency mining is not money transmission under FinCEN's regulations because a determination of whether a person is a money transmitter is based not on "the mechanism by which a person obtains the convertible virtual currency, but what the person uses the convertible virtual currency for, and for whose benefit").

[xxiii]*See* FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013) (defining an "exchanger" as a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency; and an "administrator" as a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency).

[xxiv]In the Matter of PayPal, Inc., Complaint, p. 3.

[xxv]In the Matter of PayPal, Inc., File No. 162-3102, Order, p. 8.

[xxvi]*See* Complaint, p. 4.

[xxvii]Complaint, p. 7.

[xxviii]Order, p. 9.

[xxix]Complaint, p. 11.

[xxx]Complaint, p. 12.

[xxxi]*Id.*

[xxxii]Complaint, pp. 12-13.

[xxxiii]California Civil Code § 2954.8(a) states: Every financial institution that makes loans upon the security of real property containing only a one- to four-family residence and located in this state or purchases obligations secured by such property and that receives money in advance for payment of taxes and assessments on the property, for insurance, or for other purposes relating to the property, shall pay interest on the amount so held to the borrower. The interest on such amounts shall be at the rate of at least 2% simple interest per annum. Such interest shall be credited to the borrower's account annually or upon termination of such account, whichever is earlier.

[xxxiv]*Lusnak v. Bank of America, N.A.*, No. 14-56755, p. 8 (Mar. 2, 2018).

[xxxv]15 U.S.C.A. § 1639d(g)(3).

[xxxvi]12 U.S.C.A. § 25b(b)(1)(B).

[xxxvii]*Lusnak*, p. 10.

[xxxviii]*Id.* at 11 (citing *Aguayo v. U.S. Bank*, 653 F.3d 912 (9th Cir. 2011)).

[xxxix] *Id.*

[xl] 517 U.S. 25 (1996).

[xli] *Lusnak*, p. 12 (citing *Barnett Bank*, 517 U.S. at 33).

[xlii] *Id.* at 18.

[xliii] In the Matter of The Bancorp Bank, FDIC-18-0008b and FDIC-18-0009k (Mar. 7, 2018).

[xliv] *Id.* at p. 1.

[xlv] *United States v. American Express Company*, 838 F.3d 179, 2016-2 Trade Cas. (CCH) ¶ 79766 (2d Cir. 2016), cert. granted, 138 S. Ct. 355, 199 L. Ed. 2d 261 (2017).

[xlvi] *Id.* at p. 206.

[xlvii] *Id.* at p. 196 ("The District Court's definition of the relevant market in this case is fatal to its conclusion that Amex violated § 1 [of the Sherman Act]").

[xlviii] *See generally id.* at pp. 198-200.

[xlix] *See generally id.* at pp. 202-204.

[l] *See generally Ohio v. American Express Co.,* No. 16-1454, Brief for Respondents, p. 2.

[li] *Ohio v. American Express Co.,* No. 16-1454, Brief for the Petitioners and Respondents Nebraska, Tennessee, and Texas, p. 11.

[lii] *Id.*

[liii] *Id.*

[liv] 15 U.S.C.A. § 1637(i)(2); *see also* 12 C.F.R. § 1026.9(c)(2).

FROM THE EDITORS

By Aaron Klein

This issue of the FinTech Law Report features articles by Duncan Douglass and Samuel Boro and by Lex Sokolin and Huu Nguyen.

Sokolin and Nguyen delve deeply into the world of artificial intelligence, robots and FinTech with an eye on the legal framework and structure governing this interaction. Starting off with a keen insight on the sharp generational divide regarding interacting with machine's (hint: millennials don't mind Alexa answering the phone), they move into the legal world of Robo-advisers, one of the most discussed FinTech/AI marketplaces. They examine the SEC and Finra's legal structure on robo-advising. This is followed by a brief examination of the E-sign federal legislation and the corresponding state based Uniform Electronic Transactions Act that has been adopted in 47 states.

The second article by Douglass and Boro covers the waterfront of activities occurring in the world of FinTech regulation and litigation. It begins by examining the radical changes occurring at the Consumer Financial Protection Bureau ("CFPB"). Many of the financial regulatory agencies have experienced what political insiders would consider the usual change between Democratic and Republican administration. This has not been the case at the CFPB. Instead the change has been more along the tone set by candidate and President Trump of commencing radical change on the government. Although Trump waited until a natural vacancy occurred at the CFPB, resisting calls by some to remove Director Richard Cordray, Trump's decision to appoint his chief budget staffer, Director of the Office of

Management and Budget ("OMB") Mick Mulvaney was met by immediate controversy. Even with his appointment to the dual hatted role of CFPB Acting Director and OMB Director subject to on-going legal challenge, Mulvaney has been active in re-examining and changing any and all aspects of CFPB.

Douglass and Boro begin their article by looking at the four most recent requests for information ("RFIs") on existing regulations: the CFPB's Guidance and Implementation Support; the CFPB's Financial Education Programs; and the CFPB's Consumer Complaint and Consumer Inquiry Handling Processes. This work builds on past Douglass and Boro work that examined eight earlier RFIs issued by the Bureau. The authors expect additional RFIs, and they are probably correct. Recent breaking news, is that Acting Director Mulvaney intends to also eliminate three external advisory boards: the Consumer Advisory Board, the Credit Union Advisory Council, and the Community Bank Advisory Council.

Douglass and Boro then discuss the CFPB's most recent semi-annual report to Congress that was delivered on April 1 and was the subject of congressional hearings in both the House and the Senate. Acting Director Mulvaney used the report to propose four legislative changes, which garnered both media attention and political opposition. The four changes are: (1) subjecting the CFPB to annual Congressional appropriations (the CFPB like all other bank regulators such as the Federal Reserve, FDIC, OCC are not subject to annual appropriations); (2) requiring Congressional approval of major CFPB rules; (3) ensuring that the Director answers to the President in the exercise of executive authority; and (4) creating an independent inspector general ("IG") for the CFPB (the CFPB shares the Federal Reserve's IG as technically the CFPB is part of the Federal Reserve System). While these four legislative proposals have almost no chance of being enacted into law (with the caveat of the separate IG which does have some bipartisan support) they can be taken to represent the Trump administration's official position, given Mulvaney's dual role as White House OMB Director and CFPB Acting Director.

The article flags the Federal Reserve's request for comments on changes to Regulation J, which also includes the interaction with regulation CC. The set of changes to check processing is relatively minor, given the actual changes in check processing speed and the reality of a nearly all electronic check processing world. There is an attempt to get ahead of the game by incorporating some of ISO 20022 messaging requirements.

FinCen has updated its Frequently Asked Questions (FAQs) regarding customer due diligence. Douglass and Boro cover those changes, which include new responses regarding beneficial ownership. The beneficial ownership question has recently gained some traction in Congress with bipartisan legislation proposed in both the House of Representatives by Rep. King (R-NY) and Maloney (D-NY) and in the Senate by Senators Grassley (R-IA) and Whitehouse (D-RI). This legislation has the support of several noteworthy financial services trade associations, including The Clearing House. This issue is worth keeping an eye on, especially if beneficial ownership information gains national attention in any potential scandal, as scandals often drive congressional action.

No update of the FinTech regulatory world would be complete these past few months without

a summary of the Government Accountability Office's new FinTech marketplace lending report, and Douglass and Boro deliver. For those interested in the 'sandbox' FinTech regulatory approach, taken in the UK and elsewhere abroad as well as under active consideration in several states including Arizona, the GAO report has a lengthy section dedicated to that concept.

Moving to litigation, major cases summarized include the Paypal/Venmo settlement with the Federal Trade Commission (FTC), the ninth circuit decision to unanimously allow a class action suit against Bank or America to proceed, the multi-million dollar FDIC fine against Bancorp on prepaid card fees, a new suit against Chase Bank over cryptocurrency fees for people buying Bitcoin and other crypto currencies with their credit card, and the Supreme Court oral arguments on the AmEx case.

The AmEx case decision is likely to come out in June and will be closely watched. During arguments Justices Gorsuch and Sotomayor led questions for the different sides, with Gorsuch appearing to support AmEx and question the states more aggressively, while Sotomayor did the opposite. The core issue is whether AmEx's requirement on merchants that they not allow price rebates for alternative forms of payment is anti-competitive. The article goes into detail on both the legal substance of this question and its relevance for the world of anti-trust. After all, anti-trust is the core set of precedents that this case will be decided upon and that decision may alter precedent going forward.

From a FinTech angle, the case could break new ground. The existing payment system in the U.S. is the source of much effort on the part of FinTechs. This is because the system currently does not allow price discrimination by consumers, resulting in a complex set of economic subsidies and rents for payment firms. On the consumer side wealthier consumers with fancier cards that generate higher rewards—and higher fees for merchants—are, in practice, being subsidized by lower income consumers who use less fancy credit cards, debit cards, prepaid cards, or cash. The correlation between wealth and form of payment is clear; so are the escalating set of rewards that can be thought of as tax free income.

This transfer is larger than most appreciate; a consumer, who charges $100,000 on a credit card with 1.5% being returned in cash or points, earns an additional $1,500 of post-tax income. That is probably equivalent to between $2,500 and $3,000 of pre-tax earnings depending on the consumer's tax bracket and state of residence. That is approximately 2% of the national median household income, which is just under $60,000 a year for a family of four.

If the AmEx case is decided favorably for the states, it may open the door for retailers to offer varying price incentives at the register for different forms of payment. This in turn may advantage FinTechs trying to break in to the existing payment stream but struggling to find an economic model that incentivizes both the merchant with lower payment processing costs and the consumer with greater value than existing credit card rewards. The outcome of this case may have big ramifications for FinTechs.

The article then takes an intriguing turn into an examination of robotic information and the fourth amendment. Starting with a murder investigation in Arkansas, the authors move through the relevant issues, tying the concepts into traditional bank records legal framework. While this may

sound more like the beginnings of a movie of science fiction book, recent news indicates that Amazon's Alexa and Google Home are storing vast amounts of data on speech and activity in the home. As robotic devises and artificial intelligence gains a stronger foothold into personal finance, questions of legal security and availability of data will undoubtedly follow, whether in the criminal context of money laundering or tax evasion, or in the civil space such as divorce settlements.

The article ends with a philosophical consideration of the legal and ethical considerations that may guide future policy and legal decisions as this field develops. The European context of privacy offers once such guidepost and the authors consider Articles 14 and 22 of the General Data Protection Regulation. This is a field that will likely continue to grow in importance and relevance over time.

Editorial Board

FINTECH LAW REPORT

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

FIRST CLASS
MAIL
U.S.POSTAGE
PAID
WEST

FINTECH LAW REPORT

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

THOMSON REUTERS

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

Name _____

Company _____

Street Address _____

City/State/Zip _____

Phone _____

Fax _____

E-mail _____

METHOD OF PAYMENT

❑ BILL ME

❑ VISA ❑ MASTERCARD ❑ AMEX

Account # _____

Exp. Date _____

Signature _____

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