AI and Big Data Regulatory Risks Under Banking and Consumer Financial Laws

Melanie Brody
Joy Tsai
Eric T. Mitzenmacher

Technological advancements constantly reshape America's banking and consumer finance ecosystem. Today, artificial intelligence ("AI") is among the most intriguing technologies driving financial decision-making. Powerful enough on its own to warrant significant investment, AI has even more transformative potential when coupled with industry momentum toward greater use of "big data" and alternative or non-traditional sources of information.

With material changes in banking processes on the horizon, regulators and industry participants brace themselves for the full impact of AI and big data. This article contributes to ongoing discussion by addressing the increasing regulatory focus on issues unique to, or heightened by, AI and big data. After exploring the rise of regulatory interest in these areas, we address specific regulatory risks under banking and consumer financial laws, regulations, and requirements, including: (i) the Equal Credit Opportunity Act ("ECOA") and fair lending requirements; (ii) the Fair Credit Reporting Act ("FCRA"); (iii) unfair, deceptive, and abusive acts and practices ("UDAAPs"); (iv) information security and consumer privacy; (v) safety and soundness of banking institutions; and (vi) associated vendor management expectations.

Regulators Are Increasingly Interested In AI and Big Data

As the use of AI and big data in financial services gradually becomes an industry norm, regulators have become increasingly interested and also have developed a more sophisticated understanding of the area. Federal and state regulators have now weighed in on various product types and banking processes. While doing so, they have exhibited movement from basic information gathering to a more sophisticated approach to understanding regulatory issues. Regulators have not yet promulgated material regulation specifically addressing AI and big data issues—and such active regulation appears to remain a ways off—but they have arguably moved past infancy in their approaches to such issues.

At the federal level, expressions of regulatory interest have come not only from core banking and consumer financial regulators, but also from calls by the Government Accountability Office ("GAO") for broader interagency coordination on issues related to AI and big data. The Consumer Financial Protection Bureau ("CFPB") has sought industry information on the use of alternative data and modeling techniques in the credit process in a February 2017 Request for Information,[1] and members of the Federal Reserve's Board of Governors ("FRB") have spoken on fair lending and consumer protection risks.[2] These

1 82 Fed. Reg. 1183.

2 Lael Brainard, Member, Federal Reserve Board, Speech at Fintech and the New Financial Landscape: What are we Learning about Artificial Intelligence in Financial Services? (Nov. 13, 2018) *available at*https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm.

regulators have focused, to date, on questions regarding process transparency, error correction, privacy concerns, and internalized biases, even as they see promise in AI and big data's ability to reduce lending risk and/or open credit markets to previously underserved populations. At the same time, the GAO has issued two reports (in March 2018 and December 2018) promoting or recommending interagency coordination on flexible regulatory standards for nascent financial technology ("Fintech") business models (including through "regulatory sandboxes") and the use of alternative data in underwriting processes.[3]

State regulators have also begun to involve themselves in the national discourse about AI and big data. In doing so, they have staked out similar positions to federal regulators with respect to data gathering and understanding technologies, while remaining skeptical of federal overreach in regulating (or choosing not to regulate) AI-driven processes. Various state Attorneys General, for example, have joined the discussion by opposing revisions to the CFPB's policy on no-action letters due, in part, to concern over the role machine learning could play in replacing certain forms of human interaction in overseeing underwriting questions such as "what data is relevant to a creditworthiness evaluation and how each piece of data should be weighted."[4] In addition, the New York Department of Financial Services ("NYDFS") has moved perhaps as far as any regulator—albeit in the context of life insurance, rather than banking or consumer finance—by issuing two guiding principles on the use of alternative data in life insurance underwriting: (i) that insurers must independently confirm that the data sources do not collect or use prohibited criteria; and (ii) that insurers should be confident that the use of alternative data is demonstrably predictive of mortality risk, and should be able to explain how and why the data is predictive.[5] NYDFS or other regulators may see the next logical step as applying similar requirements to the context of credit underwriting.

Not all regulatory interest is bad news for AI, big data, or the companies staking their economic futures on the two. Despite recognizing certain risks, regulators have also publicly acknowledged empirical evidence indicating potential benefits of AI and big data. The CFPB's Office of Research, for example, predicted that the use of alternative data could expand responsible access to credit to the estimated 45 million consumers who lack traditional credit scores.[6] Supporting that prediction, a white paper published by the Federal Reserve Bank of Philadelphia found statistical evidence that use of nontraditional information from alternative data sources do allow consumers with little or inaccurat credit records, based on FICO scores, to have access to credit;[7] and a study by the Federal Deposit Insurance Corporation ("FDIC") noted that one in five financial institutions cited profitability as a major obstacle to serving underbanked consumers, but that new technologies may enable consumers whose traditional accounts are

3 U.S. Government Accountability Office, GAO-18-254, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight (Mar. 2018); U.S. Government Accountability Office, GAO-19-111, Financial Technology: Agencies Should Provide Clarification on Lender's Use of Alternative Data (Dec. 2018).

4 New York Office of the Attorney General, Policy on No-Action Letters and the BCFP Product Sandbox (Feb. 11, 2019), https://ag.ny.gov/sites/default/files/cfpb_nal_and_sandbox_comment_final.pdf

5 New York Department of Financial Services Insurance Circular Letter No. 1 (Jan. 18, 2019), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2019_01

6 Consumer Financial Protection Bureau, Data Point: Credit Invisibles (May 2015), https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf

7 Federal Reserve Bank of Philadelphia, The Roles of Alternative Data and Machine Learning in Fintech Lending (Jan. 2019), https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-15r.pdf

closed for profitability issues to continue to have access to financial services.[8]

Regulators' overall attitude toward AI and big data might best be described as "cautiously optimistic." That positioning, as well as expressions of receptiveness toward further review and research, presents the industry participants with an opportunity to help construct the regulatory landscape that will ultimately govern their use of these technologies and processes. But active participation in the regulatory process requires understanding not only of the technological and business opportunities of AI and big data, but also of the legal requirements regulators are seeking to implement and/or balance.

Regulatory Issues Raised by AI and Big Data Are Diverse and Significant

As previously indicated, AI and big data have transformative potential within the banking and consumer finance industries. They are not merely incremental steps forward for credit practices, but instead are leaps toward new marketing, underwriting, and fraud and risk management approaches. Accordingly, they raise legal and regulatory issues across a variety of banking and consumer financial laws and regulatory expectations. Below, we address particular issues raised in six regulatory areas: (i) ECOA and fair lending; (ii) FCRA; (iii) UDAAPs; (iv) information security and consumer privacy; (v) safety and soundness of banking institutions; and (vi) vendor management.

ECOA and Fair Lending: Can Biases Be Controlled and Outcomes Explained?

As financial institutions increase their use of AI in marketing, underwriting, and account management activities, decision-making that is removed from—or at least less comprehensively controlled by—human interaction raises the risk of discrimination in fact patterns that courts and regulators have not previously addressed. Use of big data inputs for credit-related decision-making raises further the risk that new data points, not facially discriminatory, may be relied on by AI as proxies for protected class status.

With respect to federal consumer financial laws, ECOA prohibits a person from discriminating against an applicant on a prohibited basis regarding any aspect of a credit transaction or from making statements that would discourage on a prohibited basis a reasonable person from making or pursuing a credit application.[9] There are two theories of liability under ECOA: (i) disparate treatment, where a creditor treats an applicant differently based on a prohibited basis; and (ii) disparate impact, where a creditor uses a facially neutral policy or practice that has an adverse impact on a prohibited basis, unless the policy or practice serves a legitimate business need that cannot reasonably be achieved by another less discriminatory means. For mortgage loans, the Fair Housing Act imposes similar anti-discrimination requirements, albeit in connection with somewhat different prohibited bases.

States may also impose fair lending requirements, or even fair commerce requirements, that extend beyond lending activities. While such laws frequently protect similar classes as federal fair lending requirements do, some states add protected classes

8 Federal Deposit Insurance Corp., Assessing the Economic Inclusion of Potential of Mobile Financial Services (June 30, 2014), https://www.fdic.gov/consumers/community/mobile/mobile-financial-services.pdf

9 12 C.F.R. § 1002.4.

such as military servicemembers, or expressly protect consumers on the basis of sexual orientation in a manner that may only be implied by federal fair lending requirements.

Regulators have seized on the power of AI to detect patterns in data that may result in unlawful discrimination where traditional underwriting regimes may either have controlled more thoroughly for fair lending risk or simply not identified a pattern on which to make credit-related decisions in the first place. At a November 2018 Fintech conference on the benefits of AI, for example, Lael Brainard, a member of the FRB, noted that firms view artificial intelligence as having superior pattern recognition ability, potential cost efficiencies, greater accuracy in processing, better predictive power, and improved capacity to accommodate large and unstructured data sets,[10] but cautioned that AI presents fair lending and consumer protection risks because "algorithms and models reflect the goals and perspectives of those who develop them as well as the data that trains them and, as a result, artificial intelligence tools can reflect or 'learn' the biases of the society in which they were created." Brainard cited the example of an AI hiring tool trained with a data set of resumes of past successful hires that subsequently developed a bias against female applicants because the data set that was used predominantly consisted of resumes from male applicants. In a white paper, "Opportunities and Challenges in Online Marketplace Lending," the Treasury Department recognized this same risk, noting that data-driven algorithms present potential risk of disparate impact in credit outcomes and fair lending violations, particularly as applicants do not have the opportunity to check and correct data points used in the credit assessment process.[11]

State regulators have also focused on discrimination risk when AI and/or big data are used in underwriting or similar practices. Attorneys General of several states in an October 2018 letter to the Federal Trade Commission ("FTC") commented that the use of AI tools may lead to price-discrimination or price-targeting with negative distributional consequences for certain protected classes of consumers.[12] In addition, while in a different commercial context, the NYDFS recently issued guidance on the use of alternative data in underwriting insurance.[13] Following an investigation into insurance underwriting guidelines and practices, NYDFS identified the same concerns that federal regulators raised—the potential for violations of anti-discrimination law and the lack of transparency for consumers.

The use of AI and big data may present fair lending concerns at all phases of a credit transaction. Federal Reserve staff commented that at the credit marketing phase, the use of big data to determine what content consumers are shown may present redlining and steering risks.[14] An Internet user's web browsing history affects the advertisements he or she is shown as some companies use algorithms to send targeted advertisements. Similarly, companies could use big data to target certain groups of consumers for particular credit products. At the credit underwriting

10 Lael Brainard, Member, Federal Reserve Board, Speech at Fintech and the New Financial Landscape: What are We Learning about Artificial Intelligence In Financial Services? (Nov. 13, 2018) *available at* https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm.

11 U.S. Department of Treasury, Opportunities and Challenges in Online Marketplace Lending (May 10, 2016), https://www.treasury.gov/connect/blog/documents/opportunities_and_challenges_in_online_marketplace_lending_white_paper.pdf

12 New York Office of the Attorney General, Comment Letter on Competition and Consumer Protection in the 21st Century (Oct. 10, 2018), https://oag.ca.gov/system/files/attachments/press-docs/10.10.2018-multistate-ag-letter-ftc-re-hearings.pdf

13 New York Department of Financial Services Insurance Circular Letter No. 1 (Jan. 18, 2019), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2019_01.

14 Carol A. Evans, *Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks*, Consumer Compliance Outlook (2017).

phase, AI models may use alternative data to determine whether to grant credit or to make pricing decisions. Some data points, such as a consumer's educational background or spending habits, may have a nexus with creditworthiness but may also be correlated with race or other prohibited bases. AI algorithms could also use alternative data at the credit servicing phase to determine what modifications to offer a financially distressed consumer or when to engage in account management activities.

Regulators may expect financial institutions that use AI to implement monitoring programs to determine whether their credit models may lead to disproportionate negative effects on protected classes. The CFPB has granted a no-action letter to a company that considers educational information, in addition to traditional credit factors, in underwriting and pricing loans but has also conditioned the no-action letter with commitments to a confidential compliance plan.[15] In surveying companies that use alternative data in credit underwriting, the GAO noted that one Fintech lender monitors the effects any changes to its underwriting models may have on fair lending risk. Some of the lenders surveyed tested their credit models for accuracy, and all discussed testing to control for fair lending risk."[16]

Even in the absence of discriminatory intent or outcomes, AI may complicate compliance with technical aspects of federal and state fair lending requirements. Black box AI systems may make it difficult or impossible for certain financial institutions to comply with adverse action notice or recordkeeping requirements, for example.

With respect to required notifications, ECOA and Regulation B require that creditors provide certain notices regarding actions taken on applications for credit. Adverse action notices must contain either a statement of specific reasons for the action taken or a disclosure of the applicant's right to a statement of specific reasons taken within 30 days if the statement is requested within 60 days of the creditor's notification.[17] Whether provided upfront or only upon consumer request, a creditor's list of reasons for adverse action "must be specific and indicate the principal reason(s) for the adverse action. Statements that the adverse action was based on the creditor's internal standards or policies or that the applicant…failed to achieve a qualifying score on the creditor's credit scoring system are insufficient."[18] The regulatory language would suggest that a generic explanation such as "our proprietary algorithm for credit underwriting determined that you are ineligible" would be insufficient. In contrast, a notice indicating "your credit score is too low," but coupled with reasons for the credit score would likely be deemed sufficiently specific. The Interpretative Guidance to Regulation B further provides that specific reasons disclosed "must relate to and accurately describe the factors actually considered or scored by a creditor." If the creditor bases the adverse action on a credit scoring system, the reasons disclosed must relate only to those factors actually scored in the system. Moreover, no factor that was a principal reason for denial may be excluded from disclosure even if the relationship of that factor to predicting creditworthiness may not be clear to the applicant. Financial institutions using less transparent AI systems may find it difficult to populate an appropriate list of reasons for adverse action and

15 Consumer Financial Protection Bureau, No-Action Letter to Upstart (Sept. 14, 2017), https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter.pdf

16 U.S. Government Accountability Office, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight (Mar. 2018), https://www.gao.gov/assets/700/690803.pdf

17 12 C.F.R. § 1002.9(a)(2).

18 *Id.* § 1002.9(b)(2).

those with more transparent AI systems may find themselves responding to consumer inquiries or complaints about credit decisions made on seemingly irrelevant data points over which an AI happened to find a correlation with default rates or other material considerations.[19]

FCRA: When Is "Big Data" a "Consumer Report?"

Big data also presents risks under FCRA, and such risks are amplified if AI-driven underwriting systems have access to alternative data sources without the establishment of proper controls restricting the use of particular data elements. These risks largely relate to financial institutions inadvertently turning information into "consumer reports" under FCRA when neither the financial instruction nor the source of the data intended the data to be subject to FCRA requirements.

FCRA imposes various requirements on persons who provide "consumer reports" (i.e., "consumer reporting agencies"), as well as on persons who use or furnish information for inclusion in "consumer reports." While a traditional consumer credit report is a "consumer report," the term is far broader. Except as expressly exempted, a "consumer report" under FCRA is "the communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for determining a consumer's eligibility for credit, employment purposes, or any other purposes enumerated in the statute."[20] (The term "consumer reporting agency" somewhat circularly includes most parties who provide "consumer reports" on a for profit or a cooperative non-provider basis, so the fact that a data source does not consider itself to be a "consumer reporting agency" is not necessarily relevant to a financial institution's obligations when using alternative data.) This broad definition means that a firm that provides data that is actually used for determining credit eligibility may be subject to consumer reporting agency obligations—even if the firm did not intend for the data to be used as such.

Accidentally rendering information from a "consumer report" has a variety of regulatory consequences for a user of alternative data. For example, a consumer reporting agency may furnish (and a person may receive) a consumer report only for "permissible purposes" enumerated under FCRA. For example, a consumer reporting agency may furnish a consumer report to a person who intends to use the report in situations including: (i) in connection with a credit transaction involving the consumer, (ii) for employment purposes, (iii) in connection with insurance underwriting, or (iv) in accordance with the consumer's written instructions.[21] In many cases, entities that obtain alternative data may not have a permissible purpose. In addition, FCRA imposes an adverse action notice requirement (similar to the notice requirements under ECOA) for entities that take action with respect to any consumer that is based in whole or in part on any information contained in a consumer report.[22] Entities that use AI algorithms for credit decisions may have difficulty providing information required in FCRA adverse action notices (such as the specific source of the consumer report and the factors affecting any credit scoring model used in underwriting credit) when it is

19 FCRA also requires users of consumer reports to issue adverse action notices that include specific disclosures regarding numeric credit scores when such scores are used in deciding to take adverse action. 15 U.S.C. § 1681m.

20 *Id.* § 1681a(d)(1).

21 *Id.* § 1681b(a)(3).

22 *Id.* § 1681b(b)(3).

unclear what data points comprise of the consumer report.

Inadvertently converting a data source into a consumer reporting agency also has significant repercussions for the data source. A consumer reporting agency is subject to specific legal obligations, such as obtaining certain certifications from users of consumer reports, ensuring the accuracy of consumer information, investigating consumer disputes of inaccurate information, and filtering out certain items that cannot be reported. The GAO recognized that Fintech lenders who use alternative data in credit underwriting may have sensitive data, such as consumers' educational background or utility payment information, that may contain errors and cannot be disputed.[23]

To protect itself from becoming a consumer reporting agency (and subject to FCRA's numerous obligations), some data sources may include in their service agreements a representation that the firm will not use data for credit underwriting. If the user relies on AI models that, unknown to (or uncontrolled by) the user, pull data points from such a data source, the service agreement representation might be false. If the data used reflects on FCRA-regulated characteristics (e.g., the consumer's creditworthiness, credit standing, reputation, etc.) such that its use in credit underwriting renders the information a "consumer report," the false representation to the data source may be a false certification to a consumer reporting agency for the purpose of obtaining a consumer report. In that circumstance, in addition to possible remedies for breach of contract and regulatory action against the user, FCRA provides the consumer reporting agency a private right of action for such false representations if the representations are willful. Liability under that right of action is the greater of $1,000 or the actual damages suffered by the consumer reporting agency.[24]

Unfair or Deceptive Acts or Practices: Are AI Decisions Consistent with Disclosures?

In addition to potential ECOA and FCRA risk, an entity's use of AI and machine learning may also present risk under the catch-all prohibition against UDAAPs or, in contexts not governed by CFPB's UDAAP standards, the FTC's unfair and deceptive acts and practices ("UDAP") authority. For example, the FTC and FDIC have pursued an enforcement action against a provider of credit cards to consumers with poor credit histories for alleged violations, including a UDAP prohibition for failing to disclose to consumers that certain purchases that triggered the company's risk algorithm could reduce the consumer's credit limit.[25] The company used a behavioral scoring model that penalized consumers for using the credit card for transactions with certain merchants such as marriage counselors, automobile tire retreading and repair shops, and pawn shops. The complaint did not discuss whether certain transactions were reliably correlated with creditworthiness, but appeared more concerned with the fact that use of the behavioral scoring model was not disclosed. As black box AI systems become more prevalent, and such systems may train themselves to use novel algorithms and approaches to underwriting and account management, financial institutions may want to consider the need for broader disclaimers regarding the factors that may impact credit decisions and/or the processes that may develop new approaches to creditworthiness analysis altogether.

23 U.S. Government Accountability Office, GAO-19-111, Financial Technology: Agencies Should Provide Clarification on Lender's Use of Alternative Data (Dec. 2018).

24 15 U.S.C. § 1681n(b).

25 *Fed. Trade Comm'n v. CompuCredit Corp.*, No. 1:08-CV-1976-BBM-RGV (N.D. Ga. 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditcmplt.pdf

Information Security and Consumer Privacy: When Is Big Data Too Big?

Regulators are also aware of heightened cybersecurity and information privacy risks involved with the use of big data (whether in connection with AI-driven processes or otherwise). A GAO report explained that Fintech firms may pose consumer privacy concerns because they collect more consumer data than traditional firms. For example, firms that use alternate data in credit underwriting may have non-public personal information about consumers' educational background, bill payment history, or other sensitive data.[26] The multi-state Attorneys General in a letter to the FTC expressed concern that some firms may be accumulating big data against consumers' wishes "on account of a lack of choice and immense imbalances in market power between service providers and consumers. Consumers often concede valuable competitive data and their privacy interests because they in practice have no choice, other than foregoing the service altogether."[27] A data breach could expose sensitive personal information that consumers did not even want to share in the first place.[28] Financial institutions information security and consumer privacy practices should consider the risks raised by reliance on big data, as well as the extent to which AI-driven processes are able to seek out and utilize/store new forms of data that the financial institution otherwise does not collect.

Safety and Soundness: Can You Demonstrate Your Approach Controls Risk?

When AI and big data processes are used by banking entities, regulators have rounded out their concern about the direct effects of such processes on risk with references to general safety and soundness standards. In a Supervision and Regulation Letter, the FRB emphasized the need for critical analysis through the development, implementation, and use of models for safety and soundness.[29] A GAO report noted that the use of alternative data in underwriting decisions has not been tested in an economic downturn.[30] Some of these concerns may lessen over time, as AI approaches gain a greater history across different timeframes and fact patterns. (While some back-testing may be possible to alleviate regulators' concerns, the historic availability of alternative data with which to conduct tests across different macroeconomic climates—for example—may not be as robust as the historic availability of traditional credit data.) Until that point, however, regulators seem to expect AI risk to be monitored and controlled similarly to traditional credit practices.

Vendor Management: Can You Understand and Control Vendors' AI and Big Data Use?

Finally, beyond direct concerns as to violations of law and control of risk by financial institutions themselves, regulators have expressed interest in limiting the risk that financial institutions expose

---

26 U.S. Government Accountability Office, GAO-18-254, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight (Mar. 2018).

27 New York Office of the Attorney General, Comment Letter on Competition and Consumer Protection in the 21st Century (Oct. 10, 2018), https://oag.ca.gov/system/files/attachments/press-docs/10.10.2018-multistate-ag-letter-ftc-re-hearings.pdf.

28 On the other hand, the FRB has implicitly acknowledged the power of AI in fighting cyberattacks by suggesting that supervised institutions may need to develop their own AI tools to identify and combat outside AI-powered threats. Lael Brainard, Member, Federal Reserve Board, Speech at Fintech and the New Financial Landscape: What are we Learning about Artificial Intelligence in Financial Services? (Nov. 13, 2018) *available at* https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm.

29 Federal Reserve Board, SR Letter 11-7, Guidance on Model Risk Management (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.pdf

30 U.S. Government Accountability Office, GAO-19-111, Financial Technology: Agencies Should Provide Clarification on Lender's Use of Alternative Data (Dec. 2018).

themselves and/or consumers through partnerships with vendors who may rely on AI or big data processes. The FDIC,[31] OCC,[32] FRB,[33] and other supervisory regulators have long-expected financial institutions to control for risks involved in third-party vendor relationships and have issued guidance on effective third-party risk management. Management of vendors use of AI and big data is merely another prong in effective vendor oversight. That said, vendors may consider their systems proprietary and confidential or may otherwise maintain "black box" AI systems that cannot be fully explained. The FRB acknowledged that "it is not uncommon for there to be questions as to what level of understanding a bank should have of its vendors' models, due to the balancing of risk management, on the one hand, and protection of proprietary information, on the other. To some degree, the opacity of AI products can be seen as an extension of this balancing, but AI can introduce additional complexity because many AI tools and .models develop analysis, arrive at conclusions, or recommend decisions that may be hard to explain to regulators."[34] More concretely, NYDFS has taken the position that an insurer "may not rely on the proprietary nature of a third-party vendor's algorithmic process to justify the lack of specificity related to an adverse underwriting action,"[35] and that expectation to understand a vendor's AI models could also apply to the context of credit underwriting.

Most regulatory guidance on third-party risk management does not specifically address the challenges of understanding AI. For example, the FDIC guidance discusses risks that may be associated with third-party lending arrangements, as well as its expectation that financial institutions implement a process for evaluating and monitoring vendor relationships that include risk assessment, due diligence, contract structuring and review, and oversight.[36] However, the OCC has issued an FAQ that specifies that relationships between Fintech companies and banks may be subject to its bulletin on vendor risk management.[37] The OCC acknowledged that a bank may not be able to receive in-depth information on every third-party service provider that supports critical activities, but the OCC nonetheless expects the bank to: (i) develop appropriate alternative ways to analyze critical third-party service providers; (ii) establish risk-mitigating controls; (iii) be prepared to address interruptions in delivery; (iv) make risk-based decisions that the critical third-party vendors are the best service providers available despite the bank's inability to acquire all the information it seeks; and (v) retain appropriate documentation of efforts to obtain information.[38]

---

31 Federal Deposit Insurance Corporation, Examination Guidance for Third-Party Lending (July 29, 2016), https://www.fdic.gov/news/news/financial/2016/fil16050a.pdf

32 Office of the Comptroller of the Currency, Risk Management Guidance, 2013-29 (Oct. 30, 2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

33 Federal Reserve Board, Guidance on Managing Outsourcing Risk (Dec. 5, 2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf

34 Lael Brainard, Member, Federal Reserve Board, Speech at Fintech and the New Financial Landscape: What are we Learning about Artificial Intelligence in Financial Services? (Nov. 13, 2018) *available at* https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm.

35 New York Department of Financial Services Insurance Circular Letter No. 1 (Jan. 18, 2019), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2019_01.

36 Federal Deposit Insurance Corporation, Examination Guidance for Third-Party Lending (July 29, 2016), https://www.fdic.gov/news/news/financial/2016/fil16050a.pdf.

37 Office of the Comptroller of the Currency, Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (June 7, 2017), https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-21.html.

38 *Id.*

Conclusion

While advances in technology show a lot of promise for the financial services industry, many regulators have raised questions about responsible use from the consumer protection perspective. Regulators have developed an improved understanding of AI and machine learning, but they are also receptive to gathering more information to develop standards governing the industry. The banking and consumer finance industries are at a crucial point in the development of AI and big data processes. Careful engagement with regulatory issues raised by new technology and practices across a range of requirements and contexts will be important to the development and expansion of sustainable credit programs built around significant reliance on AI and big data.