AI Road Ahead Is Promising For Cautious Fintechs

By **Dorothy Giobbe, Alexander Maugeri and Mary Alexander Myers** (August 10, 2023)

Dorothy Giobbe

Alexander Maugeri

Mary Alexander Myers

Machine learning and artificial intelligence puts fintechs and other financial services companies at a crossroad.

These new technologies offer significant opportunity to create value for companies and consumers.

At the same time, federal and state regulators have voiced skepticism about AI across a range of areas — from bias to privacy — and government and the class action bar have broad tools to regulate its deployment. And, new congressional regulation may be on the horizon.

Recent fair lending referrals to the U.S. Department of Justice's Civil Rights Division illustrate the heightened regulatory focus — statistics released in June reflect a 90% increase since 2020, and agencies such as the Consumer Financial Protection Bureau, are increasing their "expertise in data science and analytics" to examine "[a]dvanced algorithmic technologies, as well as old technology now marketed as artificial intelligence."[1]

Despite regulatory headwinds, financial services companies have options to deploy AI in a way that mitigates risk.

To do so, they should understand the conceptions and misconceptions about AI likely to influence regulators and — before an investigation or litigation strikes — proactively study potential adverse impacts and establish use case strategies and other guardrails for deploying AI.

The Enforcement Landscape: Skepticism and New Tools

Agencies across the executive branch have made their presence known when it comes to the use of AI.

In April, the DOJ, CFPB, Federal Trade Commission and U.S. Equal Employment Opportunity Commission issued a rare joint enforcement announcement.

Though noting that AI tools "offer the promise of advancement," these financial, consumer protection and employment agencies characterized them as having "the potential to perpetuate unlawful bias, automate unlawful discrimination, and produce other harmful outcomes."[2]

This dovetails with even more blunt statements by these agency heads. For example, the FTC chair cautioned that "AI tools can turbocharge fraud and automate discrimination"[3] and the CFPB director has characterized them as "black boxes behind brick walls."[4]

In service of these goals, these agencies have asserted broad new authority.

The CFPB has authority to regulate unfair, deceptive, or abusive practices, or UDAAP.[5] The CFPB claims that it may use this authority to bring claims for discrimination, including those targeting a well-intentioned practice alleged to have a discriminatory effect on individuals in a protected group.[6]

And a March 2023 rule that the DOJ and private plaintiffs can invoke under the Fair Housing Act purports to redefine and broaden what constitutes "discriminatory effects" liability and to make it harder for courts to screen non-meritorious cases early in litigation.[7]

In the joint AI statement, the DOJ pointed to those new discriminatory effects standards as authority to regulate the output of algorithms.[8]

For its part, the FTC signaled enforcement priorities in February for AI related to marketing promises made to consumers about how AI works and collects data.[9]

In the joint AI statement, the FTC points to "combating online harms" and training algorithms based on data that should not have been collected as specific concerns.[10] This is in line with the FTC's enforcement actions involving alleged data misuse and misrepresentations with respect to AI tools, requiring remediation and reporting as well as significant civil penalties.[11]

This combination of new tools and a heightened emphasis on enforcement means that the time is now for companies in the financial services space to consider how they can capitalize on AI's promise without incurring undue risk.

How Can Financial Services Companies Respond?

The joint AI statement does more than constitute a shot across the bow.

It offers financial services companies a window into the specific areas of concern likely to arise in a lawsuit or government enforcement action. Specifically, the DOJ, CFPB, EEOC and FTC identify "data and datasets," "model opacity" and "design and use" as areas that can lead to violations of federal law.

Data and Datasets

There are two primary concerns related to data.

One is that AI tools "can correlate data with protected classes, which can lead to discriminatory outcomes."[12]

Either under its traditional anti-bias authority under the Equal Credit Opportunity Act, which prohibits discrimination against credit applicants due to race, sex, public assistance income and other bases,[13] or its newly claimed UDAAP powers over discrimination, the CFPB can investigate or litigate concerning algorithms that it perceives as having differential outcomes on protected groups.

According to the CFPB's June report to Congress, that agency has pending investigations into "potentially discriminatory conduct, including under ECOA and the statutory prohibition on unfair acts or practices targeted at vulnerable populations and leading to bias in automated systems and models."[14]

These actions can have reputational consequences for companies even if they are deemed unfounded.

To help stave this off, financial institutions and financial services companies should exercise similar caution when using AI tools developed by others as they would for technology developed in-house.

As the FTC has put it, "[i]f something goes wrong [with the AI] — maybe it fails or yields biased results — you can't just blame a third-party developer of the technology."[15] And for any AI tool, institutions should consider undertaking privileged analysis of potential correlations with race, gender, sex and other characteristics and its inputs and methodology.

Second, use of AI tools often implicates privacy issues — and these issues may soon catch the eye of state regulators enforcing recently-enacted state privacy laws.

AI tools often collect personal information from individuals and therefore, like the use of any other technology, require appropriate disclosures in privacy policies and notices. Further, the use of certain generative AI tools to produce decisions or outcomes based on personal information may require compliance with the "profiling" or "automated decision making" provisions of state privacy laws.[16]

For example, the California Privacy Protection Agency will issue a second set of regulations under the California Privacy Rights Act, part of which will focus on automated decision making.[17]

While the content of these regulations remains to be seen and enforcement may be months or even years away, the California Privacy Protection Agency will be another regulator contending with data use in AI tools.[18] Additionally, datasets used by AI may contain sensitive personal information, which may require compliance with, among other related provisions, opt-out and opt-in consent provisions of state privacy laws.[19]

Model Opacity

Because an investigation can be sparked in any number of ways — from a customer complaint to a media report — equally important is being ready for an information request, investigation or lawsuit.

This is where model opacity comes in. While the Joint AI Statement mentions drawbacks "for developers, businesses, and individuals" if a model's operation is not well understood, perhaps the most important audience for a financial services company to consider is regulators.

The reality is that if an institution cannot promptly and accurately explain how its technology works, where it obtains its data, and how privacy consents and disclosures have been managed, it runs the risk of costly and protracted investigations or enforcement actions from governmental enforcers who may assume the worst without a full picture of the technology.

If possible, financial institutions should consider going one step further. Once they know the workings of the technology, they should consider what types of experts or potential witnesses at the company would be able to articulate that in an accurate, reassuring and complete way when questions arise — whether in the form of a congressional inquiry,

financial regulatory exam or litigation.

Transparently allaying concerns early in the process can be the best way to head-off potentially disruptive matters down the line.

Design and Use

AI governance is not new — supervisory expectations are reflected in existing guidance issued by federal regulators covering such governance generally, including AI development, implementation and use; AI validation; as well as principles for governance, policies and controls.[20]

But the pace at which AI tools have developed, along with the explosion of potential applications, or use cases, has placed a renewed emphasis on AI governance, particularly with respect to those uses of AI tools that incorporate self-learning features.

Indeed, regulators are squarely focused on the potential for improper use and management of these models.[21]

Financial institutions, fintechs and companies in the financial services space should consider:

- The purpose for which AI tools are used. Those uses and risks may vary; for example, a customer-focused AI tool for credit underwriting may have greater risk considerations than an internally-focused, or back-office tool.

- Creating and maintaining an AI tool inventory — existing, planned and no longer in use — including the purpose and intended use for a given tool.

- Testing, monitoring and evaluating of the outputs and impacts of AI tools, both pre- and post-implementation.

- That monitoring AI tools alone will not fully mitigate risk: Effective data management and data governance structures, including data used to train AI tools, should be implemented. Managing data risks can also mitigate privacy and confidentiality concerns when leveraging AI tools.

- Ensuring third-party and vendor relationships are considered as part of AI governance and risk assessment. Regulators have taken the position that companies cannot outsource AI risk and compliance.

Leveraging existing control frameworks, as well as designing and implementing checkpoints

specifically relating to AI tools, can help to ensure appropriate governance in model development, deployment, ongoing use and monitoring, and throughout the model life cycle.

In many cases, companies can leverage existing compliance programs to encompass the risks of AI tools and amend such programs to cover new uses. Companies can look to some of the directives of the FTC and other agencies — including requirements of consent orders — to understand what guardrails and policies should be in place to mitigate risk of using AI tools.

The Road Ahead

In Washington, D.C., there has been recent bipartisan interest in new legislation concerning how to manage the benefits and risks of AI, especially generative AI systems.

For example, bipartisan groups of senators have discussed greater federal coordination, standards-setting or even an AI licensing regime.[22]

It would be a mistake to await potential congressional action to implement an effective AI compliance regime. As the agency initiatives underway illustrate, federal and state enforcers are not awaiting new legislation.

Additionally, one of the best ways both to influence and adapt to any future new legal landscape from Congress may be to implement robust voluntarily controls focused on understating AI inputs and outputs, eliminating model opacity and designing and implementing compliance mechanisms that mitigate risk.

In sum, if well-planned and carefully executed, embracing AI tools need not come at a hefty regulatory cost.

Dorothy Giobbe and Alexander V. Maugeri are of counsel, and Mary Alexander Myers is a partner, at Jones Day.

[1] Fair Lending Report of the Consumer Financial Protection Bureau, 88 Fed. Reg. 43087 (June 6, 2023).

[2] Consumer Fin. Prot. Bureau, et al., Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems (Apr. 25, 2023), https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf

[3] Justice Department's Civil Rights Division Joins Officials from CFPB, EEOC and FTC Pledging to Confront Bias and Discrimination in Artificial Intelligence, U.S. Dep't Just. (Apr. 25, 2023), https://www.justice.gov/opa/pr/justice-department-s-civil-rights-division-joins-officials-cfpb-eeoc-and-ftc-pledging.

[4] Remarks of Director Rohit Chopra at a Joint DOJ, CFPB, and OCC Press Conference on the Trustmark National Bank Enforcement Action, Consumer Fin. Prot. Bureau (Oct. 22, 2021), https://www.consumerfinance.gov/about-us/newsroom/remarks-of-director-rohit-chopra-at-a-joint-doj-cfpb-and-occ-press-conference-on-the-trustmark-national-bank-enforcement-action/.

[5] Dodd-Frank Act, Pub. L. 111-203, Title X, Subtitle C, Sec. 1036 (July 21, 2010).

[6] CFPB Targets Unfair Discrimination in Consumer Finance, Consumer Fin. Prot. Bureau (Mar. 16, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-targets-unfair-discrimination-in-consumer-finance. Several banking associations and business groups, in a lawsuit where a decision is expected soon, are seeking to invalidate this authority as exceeding Congress's statutory design and because of constitutional problems with how the CFPB receives its funding. See Chamber of Commerce of the United States et al. v. Consumer Fin. Prot. Bureau, Case No. 6:22-cv-00381-JCB (E.D. Tex.).

[7] Discriminatory Effects Final Rule Fact Sheet, U.S. Dept. Hous. (Mar. 17, 2023), https://www.hud.gov/sites/dfiles/FHEO/documents/DE_Final_Rule_Fact_Sheet.pdf.

[8] See generally Louis et al. v. SafeRent Solutions, LLC et al., Case No. 1:22-cv-10800-AK (D. Mass.), Doc. 37, Statement of Interest of the United States. Agreeing with many arguments advanced in DOJ's statement-of-interest brief, the district court ruled on July 26, 2023 that this lawsuit alleging discriminatory effects under the Fair Housing Act of a tenant screening algorithm could proceed to discovery. Id., Doc. 64.

[9] See Keep your AI claims in check, Fed. Trade Comm'n (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

[10] Supra n.2.

[11] See FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests, Fed. Trade Comm'n (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever; FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras, Fed. Trade Comm'n (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users.

[12] Supra n.2.

[13] 15 U.S.C. § 1691, et seq.

[14] Supra n.1.

[15] Supra n.9.

[16] California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), Civil Code Section 1798.185(a)(16); Colorado Privacy Act ("CPA"), Colorado Revised Statutes Section 6-1-1306(1)(a)(C), 6-1-1309(2)(a); Connecticut Data Privacy Act ("CTDPA"), Connecticut General Statutes Section 42-518(a), 42-522(a); and Virginia Consumer Data Protection Act ("VCDPA"), Code of Virginia Section 59.1-577(A)(5), 59.1-580(A)(3).

[17] CCPA, as amended by CPRA, Civil Code Section 1798.185(a)(16).

[18] Id.

[19] CCPA, as amended by CPRA, Civil Code Section 1798.121; CPA, Colorado Revised Statutes Section 6-1-1308(7); CTDPA, Connecticut General Statutes Section 42-520(a); Utah Consumer Privacy Act ("UCPA"), Utah Code Annotated Section 13-61-302(3); and VCDPA, Code of Virginia Section 59.1-578(A)(5).

[20] See, e,g., Guidance on Model Risk Management, Bd. of Governors of the Fed. Rsrv. Sys. & Off. of the Comptroller of the Currency (SR 11-7) (OCC 2011-12) (April 4, 2011).

[21] See, e,g., Press Release, Off. of the Comptroller of the Currency, Deputy Comptroller Testifies on Artificial Intelligence (May 13, 2022), https://www.occ.gov/news-issuances/news-releases/2022/nr-occ-2022-52.html); see also Bd. of Governors of the Fed. Reserve System, et al., Interagency Statement on the Use of Alternative Data in Credit Underwriting, (Dec. 13, 2019), https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-142a.pdf; Off. of the Comptroller of the Currency, New, Modified, or Expanded Bank Products and Services: Risk Management Principles (OCC Bulletin 2014-43) (Oct. 20, 2017).

[22] See generally U.S. Senate Hearing, Committees on the Judiciary and Homeland Security (May 16, 2023).