ICBA

One Mission. Community Banks.

August 12, 2024

Jeanette Quick
Deputy Assistant Secretary for Financial Institutions Policy
Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

RE: REQUEST FOR INFORMATION ON USES, OPPORTUNITIES, AND RISKS OF ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SERVICES SECTOR [DOC. NO. 2024-12336]

Dear Deputy Assistant Secretary Quick,

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to respond to the Department of the Treasury's Request for Information (RFI) on Uses, Opportunities, and Risks of Artificial Intelligence (AI) in the Financial Services Sector.[2] Since the launch of ChatGPT by OpenAI, there has been no shortage of public interest of artificial intelligence. At this stage, it is too early to fully predict all future use cases and consequences of AI for society and business. However, financial institutions (FI), including community banks, are beginning to explore the beneficial use cases of AI like automating manual processes, increasing the accessibility of financial services, and improving the accuracy of loan underwriting.

Like many new technologies, AI is likely to create both new risks and new opportunities for community banks. For example, while banks can use AI in transaction monitoring to identify fraudulent transactions, fraudsters can also use AI to create realistic "deepfake" audio and video that can be used to deceive financial institutions and their customers. For this reason, community banks are also carefully monitoring the development of AI technologies that can be misused to disrupt their businesses or to compromise the financial privacy of their customers.

We commend the Department of the Treasury as well as the federal financial regulators for their engagement with industry and interest in this emerging issue. In general, we do not believe that Treasury or the federal financial regulators need to issue regulations specific to AI. Regulations that are overly prescriptive may stifle the use of AI in the banking sector. Additionally, the agencies already possess a wide array of regulatory and supervisory tools that can and should be applied to the use of AI.

[1] The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at www.icba.org.

[2] 89 Fed. Reg. 50048, available at: https://www.govinfo.gov/content/pkg/FR-2024-06-12/pdf/2024-12336.pdf.

The Treasury Should Not Take a Monolithic Approach to Defining AI

> *Question 1: Is the definition of AI used in this RFI appropriate for financial institutions? Should the definition be broader or narrower, given the uses of AI by financial institutions in different contexts? To the extent possible, please provide specific suggestions on the definitions of AI used in this RFI.*

The Treasury RFI defines AI as "[a] machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments."[3] This definition resembles those developed by companies outside the financial services sector. For example, IBM defines AI as any "technology that enables computers and machines to simulate human intelligence and problem-solving capabilities."[4] Similarly, Google defines AI as "a set of technologies that enable computers to perform a variety of advanced functions."[5]

These definitions are similar in the sense that they are broad; and they capture a wide range of existing and potential technologies under the AI umbrella. Conceptually, we agree that any technology that allows computers to simulate human intelligence can be defined as artificial intelligence. However, we are concerned that this definition may be overbroad, leading to unnecessary scrutiny of basic, well-established technologies and approaches. Therefore, ICBA recommends that Treasury focuses less on a universal definition of AI, and instead, expresses AI definitions that are dependent on and derived from the specific product or service being offered.

Supervision of AI needs to be tailored to each business line, with higher risk applications receiving more scrutiny, and more routine applications receiving less. Anti-money laundering, vendor management, and similar regulations require banks to undergo robust due diligence, implement and execute comprehensive risk management strategies, continually monitor for fraud and other illicit activity, and assess credit, compliance, reputational, and legal risks. Likewise, community banks must adhere to additional compliance obligations such as those required by the Truth in Lending Act (Reg. Z), the Truth in Savings Act (TISA), the Electronic Fund Transfer Act (Reg. E), and the Expedited Funds Availability Act (Reg. CC).

If Treasury uses an overbroad definition of AI, it may have a chilling effect on the adoption of AI technologies by banks and other financial institutions. Instead, the federal bank regulators should refer to the variety of AI-related definitions listed in the National Institute of Standards and Technology's (NIST's) glossary of AI-related terms.[6] Using such definitions should enable supervision to be tailored to a community bank's particular uses of AI for different business purposes.

[3] *Id.* at 50050.
[4] IBM, "What is Artificial Intelligence (AI)," (2024), available at: https://www.ibm.com/topics/artificial-intelligence**.**
[5] Google, "What is Artificial Intelligence (AI)," (2024), available at: https://cloud.google.com/learn/what-is-artificial-intelligence.
[6] The U.S. Department of Commerce, National Institute of Standards and Technology, "Trustworthy & Responsible AI Resource Center," (2024), https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary.

Artificial Intelligence Use Cases

> *Question 2: What types of AI models and tools are financial institutions using? To what extent and how do financial institutions expect to use AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing?*

AI implements various models to assist with data collection and functionality. While this RFI does not define a model, AI models are trained on a set of data to see specific patterns or make decisions without human assistance to achieve the tasks they were created to complete. AI tools are a class of algorithms that create new text, images, or music based on the data used for tasks such as editing, making predictions and developing products.

Generative AI, which has captured significant media coverage and public interest recently, employs a statistical model that learns patterns from its training data to generate text and images in response to user prompts. However, generative AI is not the only type of AI model. AI, broadly defined, includes any process that allows computers to perform tasks that were previously thought to require human intelligence. Using this definition, AI models can range from relatively simple decision trees and static models that operate using fixed rules to more complex machine learning models that can improve themselves over time in response to new data.

Information on the expected use cases among smaller FIs is scattered; however, some smaller FIs, such as First-Foundation Bank, a California-based bank with a little over $10 billion in assets, asserts that it expects to use AI for customer service to improve bank teller lines. Additionally, FVCBankcorp, with over $2 billion in assets, has implemented an AI-driven small business lending platform where it automatically accepts or declines applications for loans and allows for approved applicants to receive funds within 48 hours.[7]

Community banks are currently using AI models in the following areas to realize cost savings and other benefits:

1) **Automating Back Office Functions:** AI is being used to automate workflows and improve fraud detection. One ICBA member bank uses AI to identify suspicious account opening activities through their online channel. The bank's CEO notes that roughly two thirds of the bank's online account opening applications are invalid and that it would take "around a dozen people to do the work that [automation and AI] do today when it comes to identifying suspicious account-opening activities."[8]

2) **Chatbots and Virtual Assistants:** Community banks are using chatbots, virtual assistants, and Intelligent Teller Machines (ITMs) to answer customer questions and provide access to bank

[7] First Virginia Community Bank, "Transforming Business Lending," (2024), available at: https://www.fvcbank.com/business-banking/lightning-lending/.

[8] *See* Elizabeth Judd, "How AI Could Help In Community Banks' Back Office," *Independent Banker* (May 8, 2024), available at: https://www.independentbanker.org/article/2024/05/08/how-ai-could-help-in-community-banks'-back-office.

services around the clock. While these innovations can decrease cost and improve accessibility, they are best used in combination with the personal service that community banks are known for and that makes relationship banking possible.

3) **Underwriting:** Some community banks have used AI models in loan underwriting – particularly in the consumer and mortgage lending space. AI-based underwriting has the potential to expand access to credit by considering more variables than traditional methods and providing a better picture of a borrower's true creditworthiness. AI-based underwriting may also increase the accuracy of loan underwriting, resulting in increased profitability and lower rates for borrowers. Despite these promises, community banks must remain mindful that AI-based underwriting must still comply with fair lending laws and that credit decisions made by AI must be explainable to the loan applicant.

4) **Cybersecurity:** AI is being used by banks to identify potential cyberattacks and to flag fraudulent emails and phishing attacks more quickly and accurately than human monitors. The ability of AI to identify patterns of suspicious network activity can help security analysts and network developers to identify malicious code. In the words of one community bank CIO, "Bad actors are already using AI for more sophisticated ingresses and breaches… Sticking your head in the sand and hoping it won't happen is not a strategy."[9]

Impact of AI on Small Financial Institutions

> *Question 4: Are there challenges or barriers to access for small financial institutions seeking to use AI? If so, why are these barriers present? Do these barriers introduce risks for small financial institutions? If so, how do financial institutions expect to mitigate those risks?*

Most financial institutions – large and small - do not typically have the resources in-house to develop cutting-edge technology, but this is most acutely felt by community banks. For example, according to a 2023 Conference of State Bank Supervisors survey, less than one percent of respondents indicated they do not rely on external providers for digital banking products and services.[10] However, reliance on third parties also invites examiner scrutiny, especially when the third party develops novel technologies, such as AI.

Examiner scrutiny has become a significant hinderance to the ability of banks to engage third parties. Aside from the actual management of the risk that these partnerships present, responding to examiner scrutiny and showing compliance with third-party risk management guidance can be prohibitive. Simply said, it is costly for community banks to ensure and demonstrate compliance with relevant regulatory requirements when selecting and monitoring third-party relationships.

[9] *See* Judith Sears, "Customers Bank's Dynamic AI Strategy," *Independent Banker* (July 15, 2024), available at: https://www.independentbanker.org/article/2024/07/15/customers-bank's-dynamic-ai-strategy.

[10] Conference of State Bank Supervisors, "Community Banking in the 21st Century: 2020 Research and Policy Conference," available at https://www.csbs.org/system/files/2020-09/cb21publication_2020.pdf

While these third parties can truly develop cutting-edge technology that can go toe-to-toe with the largest financial institutions, examiner attention to this technology can make the partnership so daunting as to not justify the risk. More than 40 percent of community bank respondents to a recent survey said the expectations of bank supervisors regarding due diligence of a third-party provider to some extent impeded the establishment of new relationships with third parties.[11] Due to this scrutiny, along with the associated costs, it is sometimes easier for banks to partner with legacy third parties that receive less scrutiny, such as core service providers.

However, the upside of partnering with a core service provider – less examiner scrutiny, and arguably, less risk – is offset by the downside limitations. There are only a handful of core service providers, creating an oligopoly market whereby the banks have limited bargaining power when negotiating service agreements. Not only can this lead to a bank that is captive to the service provider, but it can also drain monetary resources that could be better allocated to other technology providers that might better serve the community bank. Further, many core service providers, themselves, are beholden to legacy technology, making it difficult or impossible for them to develop and offer the latest technological advancements.

Actual and Potential Opportunities and Benefits of AI

> *Question 5: What are the actual and expected benefits from the use of AI to any of the following stakeholders: financial institutions, financial regulators, consumers, researchers, advocacy groups, or others? Please describe specific benefits with supporting data and examples. How has the use of AI provided specific benefits to low-to-moderate income consumers and/or underserved individuals and communities?*

The use of AI has many potential benefits for consumers, financial institutions, and financial regulators. Community banks have used AI for years in various applications ranging from fraud monitoring to underwriting. As AI technology improves, it is likely that it will play an increasingly important role in the financial services industry as both banks and their regulators use it to automate manual processes and monitor financial risks.

An additional key potential benefit of AI is that it may expand access to credit for traditionally underserved individuals and communities, including low- and moderate- income individuals and communities of color. With AI-driven models, which consider more than just credit scores, and instead incorporate alternative data that may be equally or more predictive, banks can identify credit-worthy borrowers who are not well-served by traditional underwriting. According to Louisiana State University professor Dimuthu Ratnadiwakara, "[T]he vast majority of the U.S. population—80 percent—[have] never defaulted on a loan, less than half have access to prime credit. With smarter credit models, lenders could approve almost twice as many borrowers, with fewer defaults. This could have a significant impact for both borrowers and lenders."[12]

[11] Ibid.

[12] LSU Office of Research and Economic Development, "AI and Alternative Data Could Help Millions Gain Access to Credit," (September 20, 2022), available at: https://www.lsu.edu/mediacenter/news/2022/09/wfl_lending.php.

Community banks are committed to serving their entire communities. To do this, they employ both local knowledge and personal relationships, as well as emerging technologies like AI. AI has the potential to reduce language barriers, provide better analysis of lending data, and identify unmet financial needs that community banks are well situated to serve. To the extent that AI-based underwriting reduces origination costs, it may enable more community banks to offer small dollar loans, which can be an alternative to more expensive payday and title loans for low-income customers.

Managing Third Parties

> *Question 15: To the extent financial institutions are relying on third parties to develop, deploy, or test the use of AI, and in particular, emerging AI technologies, how do financial institutions expect to manage third-party risks? How are financial institutions applying third-party risk management frameworks to the use of AI? What challenges exist to mitigating third-party risks related to AI, and in particular, emerging AI technologies, for financial institutions? How have these challenges varied or affected the use of AI across financial institutions of various sizes and complexity?*

Because banking is a regulated industry, community banks recognize that AI systems must be free of illegal bias and not lead to discriminatory outcomes.

Financial institutions may opt to use AI developed by third parties, rather than develop the approach internally. Few, if any, community banks can develop AI models in-house. Hiring programmers with the expertise required to program AI models is cost prohibitive for most community banks and the talent is not available in most regions of the country. In addition, community banks may lack the large quantities of data that are necessary to train AI models and ensure their predictive accuracy. For these reasons, partnering with third parties is the practical route for many community banks that want to develop and use AI technologies. But partnering with third parties presents certain risks that the federal banking agencies have flagged as requiring additional scrutiny. Existing agency guidance describes information and risks that may be relevant to financial institutions when selecting third-party approaches (including ones using AI) and sets out principles for the validation of such third-party approaches.

As part of an aid to those efforts, the federal banking agencies issued “Guidance on Third-Party Risk Management” (TPRM) in June 2023, a principles-based approach for managing third-party risk. Partnering with a third party does not remove or alleviate a bank’s responsibility to comply with all applicable laws and regulations, and examiners will treat a third party’s violation of law to constitute the partner bank’s violation. Banks are ultimately responsible for the actions or inactions of their third-party partners.

Community banks primarily manage their third-party risking using the framework and principles that are discussed in the Interagency Guidance on Third-Party Relationships.[13] While the Guidance is designed for general third-party risk, it is scalable, depending on the criticality or complexity of the third party and/or the third party’s product/service. Evaluating and overseeing third party providers of AI can be challenging for community banks. To alleviate this difficulty, we believe that regulators should provide

[13] 88 Fed. Reg. 37920, available at: https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf.

safe harbors for using externally developed, industry-standard AI algorithms. Standardized disclosures of how AI providers conduct their model risk assessments can be useful.
Banks typically adjust their risk-management practices based on the size, complexity, and risk profile of the third party. This assessment is conducted periodically by bank staff with the requisite knowledge and skills in each stage of the risk-management life cycle. At a fundamental level, banks are able to identify their third-party relationships, including which are critical to operations (such as processing transactions, or providing essential technology and services) or present higher risks (such as handling of sensitive data). The risk of using AI technologies will presumably hinge on its usage. In particular, if the AI technology is consumer facing, then it will likely face higher risks of imposing harm and be more closely scrutinized to protect against those risks.

We also strongly urge the agencies to utilize their offices of innovation to keep an open line of communication with community banks and to help to educate the industry. The Offices of Innovation provide significant value when researching and developing policy-based solutions that nurture bank-fintech relationships that are focused on AI. Over the past several years, the Offices have helped community banks by hosting office hours, publishing guidance on novel technologies and techniques, launching and/or considering pilot programs, initiating competitions and tech sprints, issuing advisory opinions and safe harbors for approved activities, and seeking greater information and knowledge from a wide swath of stakeholders. This effort has proven to be invaluable for community banks as they seek to forge a path for the future.

Additionally, ICBA encourages the Agencies to publish future versions of Third-Party Guidance and FAQs with opportunities for stakeholder comment, pursuant to the Administrative Procedures Act (“APA”). The notice and comment opportunity will lead to fuller consideration of any contemplated changes and will likely lead to a more robust product. For example, Question 22 in the OCC’s now-rescinded FAQs on third-party guidance is helpful insight directed toward AI usage, specifically.[14]

The FAQ highlighted principles in OCC Bulletin 2013– 29, which discussed the use of third-party models, as well as OCC Bulletin 2011–12, ‘‘Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management.’’ The FAQ provided specific guidance on third party relationships that use AI-based modeling, suggesting that if a bank lacks sufficient expertise in-house, that it could decide to engage a third party to help execute certain activities related to model risk management and the bank’s ongoing third-party monitoring responsibilities. The FAQ noted that these activities could include model validation and review, compliance functions, or other activities in support of internal audit.

Finally, the Agencies should also explore greater use of their Bank Service Company Act (BSCA) authority. BSCA provides the federal banking agencies with the authority to regulate and examine the performance of certain services by a third-party service provider for a depository institution (or for any subsidiary or affiliate of a depository institution that is subject to examination by that agency) “to the same extent as if such services were being performed by the depository institution itself on its own premises.”[15]

[14] *See* OCC Bulletin 2013-29, “Third-Party Relationship: Risk Management Guidance,” available at: https://www.occ.gov/static/rescinded-bulletins/bulletin-2013-29.pdf.
[15] 12 U.S.C. 1867(c)(1).

Explainability and Bias

> *Question 7: What challenges exist for addressing risks related to AI explainability? What methodologies are being deployed to enhance explainability and protect against potential bias risk?*
>
> *Question 10: How are financial institutions addressing any increase in fair lending and other consumer-related risks, including identifying and addressing possible discrimination, related to the use of AI, particularly emerging AI technologies?*

Using AI in underwriting has the potential to expand access to credit by identifying non-obvious patterns in data that can identify creditworthy borrowers who would be ineligible for credit using traditional underwriting techniques. The challenge with deploying this technology – and the primary reason community banks are reluctant to adopt AI as an underwriting tool – is that a machine learning algorithm that analyzes vastly more data than traditional systems and makes credit decisions that are not intuitive can be very difficult to explain. Because ECOA includes an adverse action notice requirement that includes providing applicants with the specific reasons they were rejected for a credit application, AI systems that utilize a black-box approach to underwriting may face challenges in complying with the notice requirements of fair lending laws.[16]

CFPB Circular 2023-03 attempts to answer whether creditors can rely on CFPB sample forms when providing adverse action notices relating to AI-underwritten loans. It says, "creditors may not rely on the checklist of reasons provided in the sample forms (currently codified in Regulation B) to satisfy their obligations under ECOA if those reasons do not specifically and accurately indicate the principal reason(s) for the adverse action. Nor, as a general matter, may creditors rely on overly broad or vague reasons to the extent that they obscure the specific and accurate reasons relied upon."[17]

In our view, this Circular is correct, but it creates unnecessary confusion for lenders who underwrite with AI. In no context are adverse action notices that do not provide the specific and accurate reasons for a credit denial permissible. However, we are concerned that this guidance may create the impression that the sample notification forms codified in Reg B may never be relied on with respect to AI-based underwriting.[18] This is not the case. The list of principal reasons for credit denial provided in the CFPB's sample form are all factors commonly considered in loan underwriting, whether conventional or AI-based. We believe that one or more of the denial reasons provided will be the principal reason(s) in most underwriting decisions made by AI systems, making the sample form an appropriate disclosure. Casting doubt on the adequacy of a well understood sample disclosure is likely to have a chilling effect on community banks' willingness to utilize AI.

[16] *See* 12 CFR 1002.9(b).

[17] CFPB, Circular 2023-03, Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B (September 19, 2023), available at: https://files.consumerfinance.gov/f/documents/cfpb_adverse_action_notice_circular_2023-09.pdf.

[18] *See* 12 CFR Appendix C to Part 1002.

In addition, because disparate impact liability under the fair lending laws does not require a discriminatory intent, even a facially neutral model that does not consider race or other prohibited factors can give rise to a fair lending violation if it has a discriminatory effect. The data fed into AI underwriting models may reflect historical bias, which is recreated in biased outcomes. Additionally, models may inadvertently make credit decisions using data that could be a proxy for prohibited characteristics – for example, applicants' zip codes – leading to discriminatory outcomes.

Because disparate impact violations are outcome based, the same techniques banks use to assess their compliance risks apply to both AI-based underwriting and traditional underwriting approaches. Banks can take several steps to monitor the fair lending risk of AI-based underwriting and mitigate the likelihood of committing a violation. Statistical analysis of a bank's market area may help identify potential disparate impact violations if different demographic groups have disparate approval rates or loan pricing. In addition, banks should identify any areas within their market that have a racial or national origin character and visually plot the loans they make on a map of their market to ensure those areas are being served. Failure to do so may result in a redlining violation.

Given the seriousness of fair lending violations, many banks remain uncomfortable using AI in underwriting due to the perception that it could make them more at risk. In our view, the chilling effect of disparate impact liability on the implementation of AI-based underwriting does a disservice to the very people ECOA was enacted to protect because it results in banks not using a tool that could expand access to credit to more creditworthy borrowers. Regulators can increase the lenders' willingness to use AI by providing protection from enforcement actions if lenders use AI models that are tested and proven to comply with fair lending laws. Back testing and the testing of alternative model weights are used to ensure there are no equally predictive less discriminatory alternatives (LDAs).

In 2020, the CFPB issued a No Action Letter (NAL) to Upstart Network, Inc., giving the firm a 36-month period where the Bureau will not bring a supervisory or enforcement action against upstart under ECOA or its Unfair, or Deceptive, or Abusive Acts and Practices Authority.[19] The NAL was conditioned on Upstart's adherence to a Model Risk Assessment Plan, which required the firm to provide the Bureau with model documentation on a periodic basis, test their model and/or variables or groups of variables on a periodic basis for adverse impact and predictive accuracy by group, research LDAs, and conduct periodic access-to-credit testing to determine how Upstart's model compares to other credit models in enabling credit access, along with other requirements.

We believe this NAL model has promise. Banks would feel more comfortable using AI from a third-party provider that has an NAL, or even developing their own models, if there was a clear framework for how those models are to be tested and monitored. Furthermore, the key component of the NAL model is that it provides a safe harbor from enforcement if the provisions of the Model Risk Assessment Plan are adhered to. The regulatory security this safe harbor provides would make community banks more willing to utilize AI-based underwriting, which has benefits to consumers.

[19] CFPB, Upstart Network No Action Letter (Nov. 30, 2020), available at: https://files.consumerfinance.gov/f/documents/cfpb_upstart-network-inc_no-action-letter_2020-11.pdf.

Alternative Data

> *Question 8: What types of input data are financial institutions using for development of AI models and tools, particularly models and tools relying on emerging AI technologies? Please describe the data governance structure financial institutions expect to apply in confirming the quality and integrity of data. Are financial institutions using ''non-traditional'' forms of data? If so, what forms of ''non-traditional'' data are being used? Are financial institutions using alternative forms of data? If so, what forms of alternative data are being used?*

To take advantage of the AI's ability to process vast amounts of data, banks are exploring the use of non-traditional, alternative financial data to feed AI algorithms. One of the potential benefits of using non-traditional data is providing access to credit for un- and under-banked people. Approximately 14 million Americans are unbanked, having no relationship with a bank. An additional 50 million are underbanked, meaning they have a basic relationship with a bank yet still rely on alternative financial service providers to meet their financial needs. The lack of a relationship with banks can cost consumers up to $40,000 over their lifetime in check-cashing fees and thousands more on high-interest loans from alternative providers. This means that the nearly 65 million unbanked and underbanked Americans can benefit from a more formal relationship with a community bank.

Utilizing nontraditional alternative data can help many un- and under- banked consumers establish credit history. Alternative data includes information gleaned from sources not traditionally included in a credit report, or information not customarily provided during applications for credit. This information could be generated from third parties, such as consumer reporting agencies (CRA) or data brokers, or it could be directly provided by the applicant. Examples include bank account statements, cash flow, on-time rental, utility, or telecommunications payments data (traditional credit reports typically include only late payments), or even non-financial data, such as educational history.

One of the earliest uses of alternative data was the analysis of a consumer's cash flow, which evaluates a consumer's income and expenses over time as a means to determine a borrower's ability to repay a loan.[20] Use of cash flow data is helpful for applicants that have a steady job that provides a consistent and predictable paycheck.

The federal banking agencies also see benefits from the use of non-traditional data.[21] A 2019 interagency statement noted how non-traditional data, and underlying technology that collects and makes use of the data, may improve the speed and accuracy of credit decisions and better evaluate creditworthiness of consumers who are credit invisible of those with thin credit files. This could result in the creation of additional products and/or more favorable pricing/terms.[22]

[20] FinRegLab, "The Use of Cash-Flow Data in Underwriting Credit" (February 2020), available at: https://finreglab.org/wp-content/uploads/2023/12/FinRegLab_2020-03-03_Research-Report_The-Use-of-Cash-Flow-Data-in-Underwriting-Credit_Market-Context-and-Policy-Analysis.pdf.

[21] *See* Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, "Interagency Statement on the Use of Alternative Data in Credit Underwriting" (December 2019), available at: https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-142a.pdf.

[22] Ibid.

While AI technology can help to provide an additional data-rich complement to traditional data used for credit underwriting, the agencies have also been quick to highlight the potential perils of using non-traditional data. The 2019 interagency statement cautions financial institutions to consider the impacts of their use, especially as it relates to requirements set out under ECOA and FCRA, as well as prohibitions against UDAAP.[23] However, when evaluating it through this lens, it is important to recognize that it is not the technology itself that warrants scrutiny; it is the application of the technology that needs to be evaluated.

Reliability is another potential concern when using non-traditional data. For certain sources of non-traditional data, accuracy and reliability will be relatively easy to assure. For example, data based on cash flow can be gleaned from bank account records, already tracked and accounted for, which helps ensure accuracy. Similarly, banks can easily explain how cash flow data is used to determine the ability to repay and manage their debt burdens.

Another potential risk is that many types of non-traditional data, and many of its providers, would not typically be covered by FCRA. This means that consumers might have a difficult time disputing errors that would otherwise be protected under FCRA's dispute resolution requirements.[24] Further, this data might not be as reliable because it has not been fully tested. As a GAO report found, non-traditional data might pose a risk to consumers due to inaccurate credit assessments. For example, inaccurate data or improper models might classify borrowers as higher credit risks than they actually are, resulting in unnecessarily high interest rates or the denial of creditworthy borrowers.[25]

Given the novelty and potential peril of non-traditional data, ICBA recommends that the agencies implement a trial program that grants a presumption of compliance with FCRA and fair lending laws when a positive credit decision comes from the use of non-traditional data. This should encourage its adoption, while limiting the downside risk of inadvertent discriminatory effects.

<u>AI and UDAAP Risks</u>

> *Question 10: How are consumer protection requirements outside of fair lending, such as prohibitions on unfair, deceptive and abusive acts and practices, considered during the development and use of AI? How are related risks expected to be mitigated by financial institutions using AI?*

Whether currently using, or contemplating AI, community banks evaluate a range of factors depending on how AI will be used in their institutions. For example, a community bank that is contemplating using an AI system to help create or disseminate disclosures must consider how the use may run afoul of provisions pertaining to unfair, deceptive, and abusive acts or practices. Sections 1031 and 1036 of the

[23] Ibid.

[24] CFPB, "Taskforce on Federal Consumer Financial Law Report" (January 2021), available at: https://files.consumerfinance.gov/f/documents/cfpb_taskforce-federal-consumer-financial-law_report-volume-1_2022-01_amended.pdf.

[25] Government Accountability Office, "Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight" GAO-18-254 (March 2018), available at: https://www.gao.gov/assets/gao-18-254.pdf.

Dodd-Frank Act ("DFA") forbid unfair, deceptive or abusive practices ("UDAAP").[26] Section 5 of the Federal Trade Commission Act forbids unfair or deceptive acts or practices ("UDAP").[27] An act or practice is *unfai*r if it causes or is likely to cause substantial injury to consumers that cannot be reasonably avoided, and the injury outweighs the benefits to the consumer or to competition.[28]

An act or practice is *deceptive* if it misleads or is likely to mislead the consumer and the misleading act or practice is material. [29] Under the DFA, an act or practice is abusive if it materially interferes with the consumer's ability to understand a term or condition of a consumer financial product or service, or takes unreasonable advantage of a consumer's lack of understanding of material risks, costs, or conditions; the consumer's inability to protect his or her interests; or the consumer's reasonable reliance on the provider to act in the consumer's interests.[30] A failure to disclose, or clearly disclose a material term such as an overdraft fee could lead to UDAAP/UDAP violations.

In a regulatory environment where UDAAP/UDAP violations are easy to come by, AI technology will compound an already complicated framework. Before deciding to use an AI based system to develop and disseminate disclosures a community bank would need to ensure that system is calibrated to ensure disclosure language is clear and accurate, and that they are disseminated to customers in a timely manner. Furthermore, a human monitoring component would also be needed to validate that all disclosure requirements are met. Human interaction is also necessary to allow banks to incorporate regulatory changes and new interpretations, and to ensure those changes are reflected when disclosed. In cases in which a bank has taken every step to ensure disclosure requirements are met, the slightest misstep in an AI system can render those efforts void.

Another use case that requires UDAAP/UDAP considerations is with customer facing and natural language AI systems such as chatbots. Chatbots help to ensure 24/7 support when accessing online banking services. Community banks may be inclined to implement chatbots, but not before assessing the system's ability to quickly respond to customer inquiries; the capacity for accurately processing transactions such as wires or remote deposits; ability to clearly and accurately provide explanations that respond to a consumer's specific questions; and the system's capability to be monitored by a human staff member to oversee the systems functionality and ensure consumer protection regulations are consistently adhered to. Community banks would need assurances that the AI system is accurate in all respects.

<u>Data Privacy Risk</u>

> *Question 11: How are financial institutions addressing any increase in data privacy risk related to the use of AI models, particularly emerging AI technologies? Please provide examples of how financial institutions have assessed data privacy risk in their use of AI.*

[26] Pub. L. 111-203, tit. X, sec. 1031(a), 124 Stat. 1376, 2005 (2010) (codified at 12 U.S.C. 5531(a)); see also 12 U.S.C. 5536(a)(1)(B) (making it unlawful for any covered person or service provider to engage in any abusive act or practice).

[27] 15 U.S.C. 45(a)(1)

[28] Dodd-Frank Act, Title. X, sec. 1031(c)

[29] FTC Policy Statement on Deception, available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[30] 12 U.S.C. 5531(d)(2).

Community banks are increasingly interested in leveraging AI models to enhance their services. However, they are traditionally very diligent with new technology and remain concerned about data privacy and ensuring full compliance with current privacy regulations. Fortunately, community banks have a long history of compliance with the GLBA and incorporate GLBA compliance into all aspects of any product. Furthermore, both novel products and traditional products and services leveraging AI will be closely examined for compliance with GLBA.

The industry has experience with AI and its machine learning precursor, particularly in fraud detection systems and some aspects of credit scoring models. Monitoring and analyzing transactions is one of the earliest uses of AI technology and presents a good model for privacy protection. Banks will not need to alter their approach as they adopt AI; however, certain aspects of AI may be more complex and harder to understand and explain to regulators. This might place additional emphasis on certain aspects of the already established processes.

The single most important aspect will be banks' ability to perform risk assessments of new products, involving testing and validation of data privacy risks. A complete understanding of the risks before making decisions is crucial to ensuring that GLBA compliance requirements can be met and demonstrated to regulators. Banks already heavily rely on technology service providers to deliver products and services, and AI is likely to spotlight the need for banks to understand the complete process behind a product or service. Products and services used by banks will need to be designed with GLBA compliance in mind from the outset. Additionally, technology providers must work with banks to identify any risks associated with AI so that they can properly assess and manage these risks.

Banks are proactively addressing data privacy risks associated with AI through comprehensive risk assessments, regulatory compliance, and advanced privacy technologies. Existing data privacy protections are not necessary at this time as the current GLBA requirements are flexible and sufficiently robust to ensure consumer data is protected although we acknowledge that ensuring transparency and accountability in AI usage will become more important as AI is adopted by banks.

<u>Combatting AI-Enabled Fraud</u>

> *Question 12: How are financial institutions, technology companies, or third-party service providers addressing and mitigating potential fraud risks caused by AI technologies? What challenges do organizations face in countering these fraud risks? Given AI's ability to mimic biometrics (such as a photos/video of a customer or the customer's voice) what methods do financial institutions plan to use to protect against this type of fraud (e.g., multifactor authentication)?*

Fraud is an ever-evolving problem that morphs with the adoption of new technology by banks and fraudsters alike. It is essentially a cat-and-mouse game, with each side seeking to leverage technology to meet their goals. AI can enhance fraud by making it more efficient; for example, fraudsters can use AI to write phishing emails and other communications used for fraud.

Properly authenticating customers and maintaining a robust process for this is of utmost importance to banks. A fraudster's ability to access customer accounts directly can lead to devastating consequences for both the customer and the bank where the account is held. Any development and adoption of authentication methods, especially those using biometrics that can be mimicked by AI, will need to be assessed and monitored with utmost scrutiny. Banks already use multifactor authentication; however, the methods employed will need to be consistently assessed for vulnerabilities to AI.

Community banks have not reported using potentially vulnerable biometrics for authentication; nonetheless, they will need to follow proper risk assessment procedures when adopting and monitoring the effectiveness of authentication technologies. Banks are aware of the risks posed by AI and remain vigilant in their efforts to protect their systems and customers.

AI and Illicit Finance Monitoring

> *Question 13: How do financial institutions, technology companies, or third-party service providers expect to use AI to address and mitigate illicit finance risks? What challenges do organizations face in adopting AI to counter illicit finance risks? How do financial institutions use AI to comply with applicable AML/CFT requirements? What risks may such uses create*?

While many community banks do not use AI to comply with AML/CFT requirements, the technology may offer innovative tools for streamlining compliance execution. For example, AI technology may offer enhanced monitoring and reporting by analyzing large amounts of transactional data in real time, could quickly spot behavior patterns to establish expected versus suspicious activity, and generate automated reports that respond to a specific AML/CFT regulatory requirement.

The technology could also aide in the facilitation risk assessments by reviewing numerous data points at once, such as transaction data, demographic information, product offerings, delivery channels, customer profiles, account activity, and other data points an FI deems necessary for their institution. AI based risk assessments could also lead to more efficient customer profiles, allow banks to quickly determine the level of risk it is willing to accept, allow for more effective enhanced due diligence, and automatically update when risk profiles change within an FI.

Yet, notwithstanding these potential benefits, community banks remain wary of the risks associated with its use. The technologies' ability to accurately ensure compliance with regulatory requirements is a common concern with community banks. AML/CFT compliance is regarded as one of the most consequential regulations that banks must get right at all times. Banks cannot contract away their AML/CFT responsibilities. The use of third-party providers to help facilitate compliance is met with considerable examination scrutiny as banks are responsible for the failures of the vendors they select. The use of AI technology, although potentially beneficial, may expose community banks to heightened examination scrutiny due to its novelty, the ease in which it can be manipulated, and the fact that much of the technology is not controlled by humans.

Before incorporating AI, community banks must sufficiently consider the legal, regulatory, compliance and reputational risks associated with using the technology for AML/CFT purposes. These risks are manifested through data required to build out AI models. Any bank operation system is only as good as the data used to develop that system. AI systems are no different, and in fact, the data quality is more pertinent. The efficiency of AI is largely determined by the quality of the data provided, algorithms, and on-going monitoring of these systems. If the data used to develop the model is not accurate or biased, the quality of the data will be compromised. Bad data could result in weak monitoring and ineffective reporting, thus, exposing the FI to AML/CFT deficiencies, potential findings, and fines. The quality of data could also result in profiling of certain customers potentially resulting in allegations of discrimination, result in massive de-risking, and exacerbate the number of unbanked, and underbanked consumers.

Community banks that choose to use AI for AML/CFT compliance constantly validate and monitor the data fed to the system to ensure that its use does not result in unintended risks. Community banks would also ensure there are no gaps, or opportunities for bad actors to penetrate the system by implementing a robust security apparatus designed to detect and thwart threats. To sum up the significant risk of using AI for AML/CFT compliance, there is no room for gaps or failures.

Conclusion

Once again, ICBA appreciates the opportunity to provide feedback to the Department of the Treasury pertaining to the opportunities and risks associated with the use of AI by financial institutions. We believe that AI has the potential to aid community banks in meeting the increasing burden of regulatory compliance and to expand access to credit to traditionally underserved and credit invisible borrowers. However, community banks are also aware of the risks associated with the use of AI, which range from compliance risks associated with the banks own AI use to the misuse of AI by a variety of bad actors like fraudsters and hackers.

We do not believe that Treasury or the federal financial regulators need to take additional regulatory action regarding AI at this time. Financial regulators already have a variety of technology-agnostic regulations that can be applied to AI. The same principles that govern third-party relationships, fair lending compliance, cybersecurity and privacy, and model risk management are as applicable to AI as they are to traditional approaches. Where agency action could be helpful is clarifying their supervisory expectations for AI, with specific emphasis on regulatory expectations for explainability, and by providing NALs to companies that utilize well-governed AI models in accordance with a pre-approved regulatory plan.

Please feel free to contact me at Mickey.Marshall@icba.org if you have any questions about the positions stated in this letter.

Sincerely,

M. Marshall

Mickey Marshall
AVP and Regulatory Counsel