TAKING FURTHER AGENCY ACTION ON AI

Financial Regulatory Agencies

By Todd Phillips and Adam Conner

Authors' note: *For this report, the authors use the definition of artificial intelligence (AI) from the 2020 National Defense Authorization Act, which established the National Artificial Intelligence Initiative.*[1] *This definition was also used by the 2023 "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."*[2] *Similarly, this report makes repeated reference to "Appendix I: Purposes for Which AI is Presumed to be Safety-Impacting and Rights-Impacting" of the 2024 OMB M-24-10 memo, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."*[3]

Read the fact sheet

The accompanying fact sheet lists all of the recommendations detailed in this chapter of the report.

Artificial intelligence (AI) is poised to affect every aspect of the U.S. economy and play a significant role in the U.S. financial system, leading financial regulators to take various steps to address the impact of AI on their areas of responsibility. The economic risks of AI to the U.S. financial system include everything from the potential for consumer and institutional fraud to algorithmic discrimination and AI-enabled cybersecurity risks. The impacts of AI on consumers, banks, nonbank financial institutions, and the financial system's stability are all concerns to be investigated and potentially addressed by regulators. While Governing for Impact (GFI) and the Center for American Progress have extensively researched these existing authorities in consultation with numerous subject matter experts, the goal is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. Each potential recommendation will require further vetting before agencies act. Even if additional AI legislation is needed, this menu of potential recommendations to address AI demonstrates that there are more options for agencies to explore beyond their current work and that agencies cannot and should not wait to utilize existing authorities to address AI.

The October 2023 "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" assigned executive branch financial regulators AI-related tasks[4] and specifically encouraged independent regulatory agencies, which cannot be directly tasked by the president, to address the risks of AI:

> *Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking,*

as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models.[5]

In March 2024, the U.S. Treasury Department issued a report on AI specific cybersecurity risks in financial services that included the following summary of the AI regulatory landscape:

Financial regulatory agencies generally do not issue regulations or guidance on specific technologies, but instead address the importance of effective risk management, governance, and controls regarding the use of technology, including AI, and the business activities that those technologies support. Regulators have emphasized that it is important that financial institutions and critical infrastructure organizations manage the use of AI in a safe, sound, and fair manner, in accordance with applicable laws and regulations, including those related to consumer and investor protection. Controls and oversight over the use of AI should be commensurate with the risk of the business processes supported by AI. Regulators have noted that it is important for financial institutions to identify, measure, monitor, and manage risks arising from the use of AI, as they would for the use of any other technology. Advances in technology do not render existing risk management and compliance requirements or expectations inapplicable. Various existing laws, regulations, and supervisory guidance are applicable to financial institutions' use of AI. Although existing laws, regulations, and supervisory guidance may not expressly address AI, the principles contained therein can help promote safe, sound, and fair implementation of AI.[6]

As noted in the Treasury Department's report, existing laws and regulations clearly apply to the use of AI in the financial services sector. This report for financial regulators highlights 11 relevant existing authorities and the numerous agencies that oversee them in detail below, along with recommendations on how to potentially utilize those authorities to address AI. It should be noted that there is some repetition and overlap in the recommendations for financial services regulators due to the multiple parallel existing statutory authorities. Additionally, these recommendations align with or draw from the AI best practices recommended by the Biden administration's AI Bill of Rights, the National Institute of Standards and Technology (NIST) AI Risk Management Framework, the 2023 AI executive order, and the Office of Management and Budget (OMB) M-24-10 memorandum on "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" issued in March 2024.[7]

In this report, the term "**U.S. financial regulatory agencies**" includes the federal banking and credit union agencies, financial markets regulators, and executive branch agencies. Specifically, in this report, these agencies include the Treasury Department, the Office of the Comptroller of the Currency, the Board

of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Commodity Futures Trading Commission, the National Credit Union Administration, the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau, the Financial Stability Oversight Council, which is chaired by the secretary of the treasury, and, to some extent, the Financial Industry Regulatory Authority, the self-regulatory organization for securities brokers, which is overseen by the SEC. It should be noted that other federal agencies not listed in this report also have financial regulation responsibilities and authorities that could potentially be used to address AI.

AI risks and opportunities

AI may affect financial services consumers and the U.S. and international banking and financial systems in various known and unknown ways.[8] The risks and opportunities of AI for financial services start with similar broad concerns as other areas discussed in this report, including the need for safe and secure systems with clear safeguards to address and mitigate risk, the potential for algorithmic discrimination that perpetuates or exacerbates existing historical inequalities, the potential for fraud and harm to consumers, and the possibility of affecting essential systems.

Several areas of concern are detailed below:

- **Prevention of access to financial services:** AI-powered systems may prevent consumers from accessing critical financial services[9] by illegally discriminating against customers, generating incorrect information for their credit reports, or using faulty AI systems to execute transactions. The OMB M-24-10 AI guidance lists AI used by federal agencies for "[a]llocating loans; determining financial-system access; credit scoring; determining who is subject to a financial audit; making insurance determinations and risk assessments; determining interest rates; or determining financial penalties" as potentially rights-impacting.[10]

- **Algorithmic discrimination that may exacerbate historical inequalities:** Massive amounts of data are required to train and run AI-powered systems.[11] In the financial services world, such historical data may dangerously reflect long-embedded systemic inequalities, such as redlining, unfair credit denials, and other discriminatory practices. AI systems trained on these historic data run the substantial risk of incorporating these inequities if not addressed proactively.

- **AI-enabled fraud:** AI is already embraced as a tool to enable advanced fraud against consumers and financial institutions. The use of AI voice cloning[12] and AI-generated fake accounts[13] are just the tip of the iceberg when it comes to future AI-enabled financial fraud.

- **Failure to comply with anti-money laundering requirements:** The Bank Secrecy Act and Treasury Department regulations require institutions to submit suspicious activity reports (SARs) whenever customers engage in activity that may be money laundering.[14] Black-box AI systems may fail to report otherwise suspicious activities, leaving banks in violation of the Bank Secrecy Act.

- **Threats to safe, secure, and stable financial systems:** Integrating AI systems into financial services may pose a risk to the operation of these critical systems, as their sophistication grows along with the lack of transparency into proprietary black-box AI systems and algorithms that provide essential services and upkeep. The 2008 financial crisis proved how important the stability of the broader financial system is for a growing economy; yet AI and the commercial cloud computing that provides advanced AI pose risks that could negatively affect financial stability. Indeed, the Financial Stability Oversight Council has identified AI as a "vulnerability" within the U.S. financial system.[15] For example, a bank's use of the same or similar data for AI-based risk management models, AI-enabled network effects, or unregulated AI service providers may pose systemic risks.[16]

Although certainly not exhaustive, these known risks affect at least three main categories of stakeholders in the financial sector:

1. **Customers:** Banks and other financial services providers may illegally discriminate against customers when making lending decisions with unknowingly biased AI systems.[17] Banks' and lenders' retail and institutional customers are also at risk of faulty AI systems that fail to accurately respond to their inquiries, accurately assess their credit worthiness, or execute transactions.[18] Similarly, brokers' customers face losses from transactions that AI systems fail to execute.[19] Financial institutions also serve as a wealth of information about customers, which is necessary for AI systems to operate, and may be liable for customer losses stemming from AI-enabled fraud.[20]
2. **Banks:** The core purpose of bank regulation is to ensure banks' safety and soundness,[21] and AI could put this at risk. Banks face potential operational failures from AI-enabled cyberattacks that can evade their information technology (IT) defenses,[22] runs from depositors' use of AI for treasury management,[23] and losses from banks' own opaque and faulty AI-based risk management systems.[24]
3. **Securities brokers and futures commission merchants, securities and derivatives exchanges, and other market intermediaries:** In addition to banks, the nonbank financial institutions that comprise the capital markets are also poised to use AI systems that may pose risks to firms' financial health and that of markets overall. Brokers may be liable for trades that AI systems failed to execute or misexecuted, and investment advisers and brokers may be liable for AI systems that fail to offer conflict-free advice or advice in the clients' best interests.[25] Exchanges may face operational failures from their AI-based

matching software or experience flash crashes stemming from erroneous high-frequency trading.[26] Additionally, clearinghouses relying on AI systems that fail may be unable to novate trades, putting the markets at risk of requiring bailouts.[27]

Current state

The 2022 White House AI Bill of Rights, which was the basis of much of the 2023 executive order on AI, noted that AI or automated systems could "have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services" and that critical resources or services included financial services.[28]

The 2023 AI executive order outlines eight policies and principles for AI for the Biden administration's approach to AI, including that AI must be "safe and secure," "[promote] responsible innovation, competition, and collaboration," and "[advance] equity and civil rights," as AI "systems deployed irresponsibly have reproduced and intensified existing inequities, caused new types of harmful discrimination, and exacerbated online and physical harms." The guidance specifically highlights the need to "enforce existing consumer protection laws and principles and enact appropriate safeguards against fraud, unintended bias, discrimination, infringements on privacy, and other harms from AI," emphasizing the need for protections in "financial services."[29]

The executive order also required the secretary of the treasury to "issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks" and provides financial services and housing directives for the CFPB.[30] Finally, the order highlights the direction it hopes independent regulatory agencies not under the direct authority of the president will take on AI, noting:

> *Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models.*[31]

The OMB M-24-10 AI guidance notes that AI used by federal agencies should be automatically presumed rights-impacting if used for "[a]llocating loans; determining financial-system access; credit scoring; determining who is subject to a financial audit; making insurance determinations and risk assessments; determining interest rates; or determining financial penalties (e.g., garnishing wages or withholding tax returns)."[32]

The financial regulatory agencies have been working on addressing AI in a variety of ways.

The Consumer Financial Protection Bureau (CFPB) has been one of the most proactive federal agencies on the issue.[33] Director Rohit Chopra has made statements warning about the myriad risks of AI, including that its need for large datasets and computing power could result in a natural oligopoly: "There could be a handful of firms, and just to be honest, a handful of individuals who ultimately have enormous control over decisions made throughout the world."[34] Chopra has also expressed concern that AI "magnifies disruptions in a market that turn tremors into earthquakes"[35] and that AI could be used for illegal and discriminatory lending decisions.[36]

Accordingly, the CFPB has provided market participants with various guidance about how AI may and may not be used. The CFPB explained that federal law does "not permit creditors to use complex algorithms when doing so means they cannot provide the specific and accurate reasons for adverse actions."[37] It has also warned that creditors may not "rely on overly broad or vague reasons to the extent that they obscure the specific and accurate reasons relied upon."[38] The CFPB has criticized credit reporting agencies' use of AI screening tools.[39] In conjunction with the U.S. Department of Justice, Equal Employment Opportunity Commission, and Federal Trade Commission, the CFPB warned that AI systems "have the potential to produce outcomes that result in unlawful discrimination" and that "[e]xisting legal authorities apply to the use of [AI] just as they apply to other practices."[40] The CFPB has also penalized firms for relying on faulty automated compliance systems. The bureau ordered Wells Fargo to pay $3.7 billion for compliance failures that resulted in wrongful home foreclosures, car repossessions, and lost benefit payments[41] and ordered Hello Digit to pay a $2.7 million fine for causing users to be charged overdraft fees.[42] It is reportedly increasing examinations of AI systems.[43]

At the Treasury Department, Graham Steele, while serving as assistant secretary for financial institutions in October 2023, gave a speech detailing how AI can affect banking, consumer finance, and insurance markets and emphasizing the importance of AI providers engaging in responsible innovation.[44] In addition, the Treasury Department appointed a chief artificial intelligence officer as required by the 2023 executive order on AI.[45] The Financial Stability Oversight Council (FSOC), which is chaired by the treasury secretary, has identified AI as a potential risk to the financial system and has issued recommendations to the other regulators to monitor AI's development in their respective jurisdictions.[46] In a February 2024 testimony before the U.S. House Committee on Financial Services, Treasury Secretary Janet Yellen noted that the FSOC was "closely monitoring the increasing use of artificial intelligence in financial services, which brings potential benefits such as reducing costs and improving efficiencies and potential risks like cyber and model risk."[47] And in March 2024, the Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection issued a report in response to requirements

from the 2023 executive order on AI, entitled "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector."[48] While focusing on the AI-specific risk of cybersecurity, the "Next Steps: Challenges & Opportunities" chapter contains a small section that notes "Regulation of AI in Financial Services Remains an Open Question" according to those interviewed for the report.[49]

The federal banking agencies have also begun tackling AI, albeit at a slower pace.[50] The Office of the Comptroller of the Currency (OCC) formed an Office of Financial Technology.[51] The Federal Deposit Insurance Corporation (FDIC) created FDITech, a tech lab, though it recently reduced its public-facing role.[52] Four federal reserve banks—San Francisco, New York, Atlanta, and Boston—have also set up offices to study financial innovation and AI.[53] These efforts are intended to focus, in part, on how regulators can use AI to assist in regulating financial institutions as well as to better understand how banks are using AI in their activities. These agencies have also jointly issued a request for information on financial institutions' uses of AI[54] and have proposed a rule to impose heightened standards for the use of home appraisals conducted using algorithms.[55]

The Securities and Exchange Commission (SEC) is quickly evaluating how regulated institutions use AI in capital markets. Chairman Gary Gensler has given a plethora of speeches discussing the possible harms of AI,[56] including in a March 2024 interview with Politico in which he warned of a potential financial crisis caused in part by AI.[57] In addition, the agency has launched a Strategic Hub for Innovation and Financial Technology (FinHub) that focuses, in part, on AI generally in the securities markets.[58] The SEC proposed a rule to address risks posed to investors from conflicts of interest associated with using predictive data analytics.[59] With regard to investment advisers, the SEC's examinations division has begun soliciting information about advisers' uses of AI.[60] SEC staff have issued guidance[61] and a risk alert[62] addressing robo-advisers that use algorithms to make investment recommendations.

The Financial Industry Regulatory Authority (FINRA), the self-regulatory organization for securities brokers,[63] formed an Office of Financial Innovation to coordinate fintech efforts that include AI[64] and published a white paper on AI in the securities industry.[65]

The Commodity Futures Trading Commission (CFTC) issued "A Primer on Artificial Intelligence in Financial Markets" in 2019 that discusses, among other things, how the CFTC could leverage AI to better regulate its markets.[66] More recently, the agency created an enforcement division task force focused on emerging technologies, including AI,[67] and its Technology Advisory Committee created a panel to evaluate "responsible artificial intelligence."[68] The CFTC's commissioners have given speeches on the need for the agency to regulate AI.[69]

The Biden administration's work on AI is ongoing, but the AI Bill of Rights, the NIST AI Risk Management Framework, the 2023 executive order on AI, and the OMB M-24-10 AI guidance have highlighted key AI risk mitigation practices to be further developed.[70] Due to parallel statutory authorities across multiple agencies, many of these recommendations are referenced repeatedly in the sections below.

These efforts include, but are not limited to, the following:

- **Required minimum risk management practices for AI use that is deemed safety-impacting or rights-impacting:** The OMB M-24-10 AI guidance requires minimum risk management practices for federal agencies that utilize AI for certain purposes presumed to be safety-impacting or rights-impacting.[71] These steps, including AI impact assessments and other requirements, could be repurposed for use beyond federal agencies, such as at banks or financial services institutions.

- **AI audits:** The development of an independent third-party AI auditing ecosystem is being explored to ensure effective risk management and compliance with AI systems.[72] AI audits in this context can include both the data used to train AI systems and the AI systems themselves, including their source code. The audits would also include third parties utilizing AI for banks or other financial institutions as vendors or contractors. In all cases, regulators should set out guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Explainability and legibility:** The 2022 AI Bill of Rights[73] made "notice and explanation" a key principle for the safe use of AI, noting that people "should know that an automated system is being used and understand how and why it contributes to outcomes that impact you" and that automated systems should "provide clear, timely, understandable, and accessible notice of use and explanations."[74] The 2023 AI executive order noted that "requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models" should be a priority for independent agencies, including independent financial regulators.[75] This expectation for explainability and legibility is also reflected in the OMB M-24-10 AI guidance for federal agencies using or procuring AI, which notes:

  > *Explanations might include, for example, how and why the AI-driven decision or action was taken. This does not mean that agencies must provide a perfect breakdown of how a machine learning system came to a conclusion, as exact explanations of AI decisions may not be technically feasible. However, agencies should still characterize the general nature of such AI decisions through context such as the data that the decision relied upon, the design of the AI, and the broader decision-making context in which the system operates. Such explanations should be technologically valid, meaningful, useful, and as simply stated as possible, and higher-risk decisions should be accompanied by more comprehensive explanations.*[76]

Financial regulators should collaborate with others in the public and private sector as they develop best practices for explanation and legibility.

- **AI red-teaming:** The 2023 AI executive order defined AI "red-teaming" as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[77] Red-teaming has emerged as a method to test AI that is embraced by leading generative AI companies[78] and has been a focus of the White House in voluntary commitments,[79] the executive order, and the OMB M-24-10 AI guidance.[80] This can also include red team/blue team exercises, whereby the blue team defends the systems against the simulated penetrations,[81] or "violet-teaming," which attempts to address broader systemic societal issues in adversarial testing.[82]

- **Cybersecurity and AI risk management:** The Biden administration has made cybersecurity a key focus, with efforts that include the 2023 National Cybersecurity Strategy.[83] The 2023 executive order on AI also prominently mentions cybersecurity throughout. Similarly, AI risk management has been an early focus of voluntary and mandated AI efforts from the U.S. government, including the NIST AI Risk Management Framework and the OMB M-24-10 AI guidance.[84]

Relevant statutory authorities

This section explains how various statutes enforced by the federal financial regulators could be used to regulate AI. This list is by no means exhaustive.

Bank Secrecy Act

Relevant agencies: *Treasury Department, Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission*

The Bank Secrecy Act (BSA), enacted in 1970, is designed to combat money laundering and financial crimes.[85] The BSA and regulations promulgated thereunder require financial institutions to maintain records and report certain transactions indicative of money laundering or other illicit activities.[86] Under these regulations, banks and other financial institutions must verify the identity of all customers, keep detailed records of cash transactions exceeding $10,000, and report suspicious transactions to the Financial Crimes Enforcement Network (FinCEN).[87] By mandating these reporting requirements, the BSA aims to enhance transparency in financial dealings, detect potential illegal activities, and safeguard the financial system's integrity.[88]

The broad statutory authority allows the treasury secretary and banking and financial regulators to promulgate regulations requiring institutions to create and implement a wide variety of anti-money laundering programs.[89]

Recommendations

Using these authorities, the Federal Reserve, OCC, FDIC, SEC, and CFTC could consider the following actions:

- **Regulate how institutions' customer identification and suspicious activity reporting programs use AI.** As AI becomes more integrated into financial systems, it can help institutions monitor and analyze transactions for BSA compliance more effectively, detecting anomalies or patterns indicative of illicit activities. However, regulators must be cognizant of the harms of offloading such an important law enforcement task to AI systems and should outline best practices for implementing AI systems and require institutions to develop standards for how they use AI to automate anti-money laundering tasks.

- **Require banks to periodically review their BSA systems to ensure accuracy and explainability.** Accurate and timely reports of suspicious activities must be balanced against financial privacy and FinCEN's ability to review the reports it receives. Regulators must ensure the AI institutions' BSA systems use is accurate and can explain why activities are suspicious and therefore flagged. Regulators should require institutions to periodically review their AI – perhaps by hiring outside reviewers – to ensure continued accuracy and explainability to expert and lay audiences. Examiners must be able to review source code and dataset acquisition protocols.

Gramm-Leach-Bliley Act: Disclosure of nonpublic personal information

Relevant agencies: *Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission, Consumer Financial Protection Bureau*

Enacted in 1999, the Gramm-Leach-Bliley Act (GLBA) proclaimed it "the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[90] Accordingly, 15 U.S.C. § 6802 provides that "a financial institution may not … disclose to a nonaffiliated third party any nonpublic personal information" unless it has first provided consumers notice.[91]

The GLBA requires the banking and financial regulators to "establish appropriate ... administrative, technical, and physical safeguards" for institutions that 1) "insure the security and confidentiality of customer records and information"; 2) "protect against any anticipated threats or hazards to the security or integrity of such records"; and 3) "protect against unauthorized access to or use of [customer information]."[92] Under this authority, the federal banking regulators have implemented interagency guidelines for establishing information security standards[93] and issued IT and cybersecurity risk management guidance.[94]

Recommendations

The regulators should make further use of this authority to ensure resiliency against AI-designed cyber threats, including the following actions:

- **Require third-party AI audits for all institutions.** AI audits should be required for all institutions. Larger institutions can bring this practice in-house, depending on the ecosystem that develops around AI audits. However, smaller financial institutions may lack the staff and funding for in-house expertise or AI red-teaming but still need to mitigate against AI risk. Accordingly, small institutions should undergo AI security audits by qualified outside consultants to determine where vulnerabilities lie. These audits help identify and address any vulnerabilities in AI systems that might be exploited by cyber threats, thus enhancing overall cybersecurity measures. This includes risks that cybercriminals could use AI to impersonate clients such that institutions inadvertently release customer information erroneously, believing that they are interacting with their clients. Regulators should set out guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Require red-teaming of AI for the largest institutions.** AI red-teaming is defined as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[95] The largest firms should already be utilizing red-teaming for their AI products. In addition, they should be running red team/blue team exercises, and the agencies should require the teams to incorporate AI into their efforts. Using AI can significantly increase the speed at which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[96] Firms must know how malicious actors can use AI to attack their infrastructure to defend against it effectively. Banks and other financial institutions must conduct AI red-teaming to fortify their cyber defenses and proactively identify vulnerabilities.

- **Require disclosure of annual resources on AI cybersecurity and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the

escalating reliance on AI-driven technologies in banking operations, the potential vulnerabilities and risks associated with cyber threats amplify significantly. By mandating such disclosures, stakeholders, including customers, regulators, and investors, gain valuable insights into a bank's commitment to mitigating cyber risks through AI.

Equal Credit Opportunity Act

Relevant agency: *Consumer Financial Protection Bureau*

The Equal Credit Opportunity Act (ECOA) was enacted to prevent discrimination in credit granting. The ECOA makes it "unlawful for any creditor to discriminate against any applicant" for credit "on the basis of race, color, religion, national origin, sex or marital status, or age" or "because all or part of the applicant's income derives from any public assistance program."[97] The ECOA requires creditors to provide reasons for credit denials and grants applicants the right to challenge any decision perceived as discriminatory. Its fundamental goal is to promote fair and equal access to credit for all qualified individuals, fostering a more inclusive and equitable financial landscape.

The ECOA allows the Consumer Financial Protection Bureau to "prescribe regulations to carry out the purposes of [the act]," including those it believes "are necessary or proper to effectuate [the ECOA's purposes], to prevent circumvention or evasion thereof, or to facilitate or substantiate compliance therewith."[98] It also requires firms to provide "[e]ach applicant against whom adverse action is taken [with] a statement of reasons for such action."[99]

Recommendations

Using these authorities, the CFPB could consider the following actions:

- **Require lenders to periodically review their lending systems to ensure explainability and that no new discriminatory activity applies.** Research suggests that AI-based systems may result in lending decisions that have a disparate impact,[100] which is a violation of the ECOA.[101] The CFPB has already indicated in guidance that AI-based lending systems cannot be used when those systems "cannot provide the specific and accurate reasons for adverse actions."[102] Nevertheless, the CFPB should require lenders making lending decisions using AI to periodically review those systems – perhaps by hiring outside reviewers – to ensure explainability to expert and lay audiences and to confirm that discrimination does not inadvertently creep in as new data are used. Examiners must review source code and dataset acquisition protocols.

- **Prohibit lenders from using third-party credit scores and models developed with unexplainable AI.** Many lenders use credit scores or other sources of information from third parties, which themselves may use AI to create those ratings.[103] The CFPB should prohibit lenders from using unexplainable scores or models to avoid fair lending requirements and require all lenders subject to the ECOA to obtain information about the explainability of their third-party service providers' AI.

- **Require lenders to employ staff with AI expertise.** As described above, many lenders rely on third-party models for lending decisions. Given the pitfalls of algorithmic lending decisions, these firms must maintain diverse teams that include individuals with AI expertise to understand how such models operate and can introduce bias into firms' lending decisions. These experts are necessary to identify and mitigate potential biases or unintended consequences of algorithmic decision-making. The 2023 executive order on AI required federal agencies to appoint chief artificial intelligence officers (CAIOs),[104] whose duties were further outlined in the OMB M-24-10 AI guidance.[105] The CFPB should follow that model to require firms to similarly designate a CAIO or designate an existing official to assume the duties of a CAIO.

Fair Credit Reporting Act

Relevant agency: *Consumer Financial Protection Bureau*

Recognizing that "the banking system is dependent upon fair and accurate credit reporting" and that "inaccurate credit reports directly impair the efficiency of the banking system," Congress enacted the Fair Credit Reporting Act (FCRA) in 1970.[106] The FCRA generally covers all entities that help create, provide, and use consumer reports and allows the Consumer Financial Protection Bureau to regulate those activities. For example, the FCRA prohibits entities that furnish information to consumer reporting agencies (CRAs) from reporting information that they know have errors, mandating they correct and update false information, and allows the CFPB to craft regulations prescribing policies and procedures that must be followed.[107] For CRAs themselves, the FCRA excludes particular information from reports and requires agencies to describe to users the key factor in credit score information.[108] And for users of consumer reports—which include lenders, employers, and landlords—the FCRA prescribes responsibilities if they take adverse actions based on report information and allows the CFPB to regulate how users provide consumers with credit decision notices and the information contained in such notices.[109] The CFPB may also regulate the procedures for instances where consumers wish to dispute the accuracy of information in reports.[110] The Federal Trade Commission, CFPB, and other agencies have administrative enforcement authority.[111]

Using this regulatory authority, the CFPB has issued regulations creating and requiring firms to use model forms and disclosures,[112] requiring furnishers of information to "establish and implement reasonable written policies and procedures regarding the accuracy and integrity of the information [provided to credit reporting agencies]],"[113] and requiring users of credit reports to disclose to consumers when their credit report has been used as a means for determining their risk.[114]

Recommendations

As it relates to AI, the CFPB should consider using these authorities to take the following actions:

- **Require credit reporting agencies to describe whether and to what extent AI was involved in formulating reports and scores.** Although the CFPB has issued guidance making clear that the ECOA requires lenders to make their AI systems explainable,[115] it has yet to do the same with credit reporting agencies. Given that AI-based systems may result in the creation of credit scores that will result in a disparate impact, the CFPB should use its authority over credit reporting agencies to make clear that the AI used to generate credit scores should describe the extent to which AI was used and ensure the scores are explainable.

- **Require credit reporting agencies to periodically review their AI systems to ensure explainability and that no new discriminatory activity applies.** Beyond simply requiring credit reporting agencies' AI systems to be explainable to expert and lay audiences, the CFPB should also require the agencies to periodically review their systems to ensure continued explainability as new data are introduced. CFPB examiners must be able to review source code and dataset acquisition protocols.

- **Require credit reporting agencies to provide for human review of information that consumers contest as inaccurate.** As part of U.S.C. § 1681i "reasonable reinvestigation" mandate, credit reporting agencies should be required to have a human conduct the reinvestigation of AI systems' determinations and inputs.[116] Since AI-based systems may use black-box algorithms to determine credit scores or inputs that create credit scores, individually traceable data are required for adequate human review. As noted above, general explainability is important but would not be sufficient to allow human reviewers to correct potentially erroneous information under the FCRA.

- Given the preceding recommendation, **require users of credit reports to inform consumers of their right to human review of inaccuracies in AI-generated reports in adverse action notices**, per 15 U.S.C. § 1681(m)(4)(B).

- **Update model forms and disclosures to incorporate disclosure of AI usage.** Given the CFPB's mandate that credit reporting agencies and users of credit reports use model forms and disclosures, the CFPB should update those forms to include spaces for model form users to describe their AI usage.

Importantly, "consumer reports" under the FCRA include those that provide information used "in establishing the consumer's eligibility for ... employment purposes."[117] "Employment purposes" includes the "purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee."[118] The CFPB should consider several policy changes to explicitly address electronic surveillance and automated management (ESAM) used by employers:

- **Require purveyors of workplace surveillance technologies to comply with the FCRA.** As AI firms become increasingly used to mine data provided by employers, it is important that ESAM software companies be considered credit reporting agencies and comply with the corresponding restrictions. The CFPB should consider adding such companies to its list of credit reporting agencies[119] and issue supervisory guidance explaining the circumstances under which ESAM companies act as CRAs and the corresponding responsibilities that they entail for ESAM companies and employers.

- **Ensure ESAM technologies used by employers comply with the FCRA.** If the CFPB provides that these technology providers are CRAs, the CFPB must also make clear that users of their software comply with the FCRA. Accordingly, it should consider modifying the "Summary of Consumer Rights" issued by the CFPB to include information about employee FCRA rights concerning employers' use of ESAM technologies.[120] It should also consider modifying "Appendix E to Part 1022" to identify how employers furnishing employee data to ESAM technology companies and data brokers must ensure the accuracy of their furnished information.[121]

Community Reinvestment Act

Relevant agencies: *Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation*

Enacted to undo the pernicious effects of redlining,[122] the Community Reinvestment Act (CRA) encourages banks to meet the credit needs of the communities in which they operate, particularly low- and moderate-income neighborhoods. The CRA requires banks to actively engage in lending, investment, and service activities in these underserved communities by mandating periodic evaluations of banks' performance in meeting the community's credit needs.[123] The CRA grants federal banking regulators the authority to regulate banks' compliance with the law.[124]

The CRA does not allow regulators to change banks' lending decisions, only to decide how it will evaluate whether banks comply with the act. The regulators' rules allow banks to submit strategic plans for complying with the CRA[125] and establish assessment areas for determining compliance.[126]

Recommendation

The federal banking regulators should consider using their authority to:

- **Require banks to indicate whether they use AI to comply with CRA regulations and, if so, require those systems to be explainable.** Given AI systems' abilities to wade through mountains of information and identify the most profitable outcomes, banks may use them to game CRA regulations. For example, banks may use AI to help determine the most optimal assessment areas for profitability purposes. Regulators should require banks to disclose if they use AI to comply with the CRA or with regulations promulgated thereunder. In addition, these AI systems should be required to be explainable to expert and lay audiences to ensure that designated assessment areas are logical. Examiners must be able to review source code and dataset acquisition protocols.

Consumer Financial Protection Act: UDAAP authority

Relevant agency: *Consumer Financial Protection Bureau*

Following the great financial crisis of 2007–2008, Congress enacted the Consumer Financial Protection Act (CFPA) as Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. Among other things, the CFPA created the Consumer Financial Protection Bureau to ensure fairness, transparency, and accountability in providing consumer financial products and services by regulating those products and services and enforcing the nation's consumer financial protection laws.[127] The Consumer Financial Protection Bureau regulates various financial sectors, including banks, credit unions, mortgage servicers, payday lenders, and debt collectors, striving to educate consumers and monitor financial practices.

One of the most potent authorities provided to the CFPB is its authority to "take any action authorized ... to prevent a covered person or service provider from committing or engaging in an unfair, deceptive, or abusive act or practice under Federal law in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service."[128] Under this so-called UDAAP authority, the CFPB may also write regulations "identifying as unlawful" particular acts or practices and "may include requirements for the purpose of preventing such acts or practices."[129] In other words, the CFPB can regulate consumer financial service providers to ensure their activities are not unfair, deceptive, or abusive.

Recommendations

Using this authority, the CFPB should consider the following actions:

- **Require financial institutions' consumer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict consumer protection standards, periodically reviewing consumer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems must provide consumers with accurate information about their accounts, their firms' policies and procedures, and the law. In addition, as these AI systems begin to be used for more than simply providing information – such as executing customers' money transfers or asset purchases – it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and comply with firms' policies. The CFPB must ensure that institutions' consumer-facing AI systems are accurate in all respects and require, through rulemaking, periodic review of their systems to ensure accuracy.

- **Require AI red-teaming and red team/blue team exercises for the largest institutions.** The CFPB's UDAAP authority can be used to prohibit the inadvertent disclosure of consumers' information at institutions not subject to the GLBA.[130] Nonbank consumer financial service providers hold a wealth of information about customers that malicious AI systems feed off, and they may be liable for customer losses stemming from AI-enabled fraud.[131] With AI red-teaming[132] or red team/blue team exercises, the red team attempts to attack a company's information technology infrastructure while the blue team defends against such hacks. The largest firms should already be utilizing AI red-teaming and red team/blue team exercises, but given that real-world attackers have AI at their disposal, the agencies should require this. Having teams use AI can significantly increase the speed with which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[133] Firms must understand how malicious actors can use AI to attack their infrastructure and defend against it. Institutions must conduct AI red-teaming and red team/blue team exercises leveraging AI to fortify their cyber defenses and proactively identify vulnerabilities.

- **Require third-party AI audits for all institutions.** AI audits should be required by all institutions. Larger institutions can bring this practice in-house, depending on the ecosystem that develops around AI audits. However, smaller financial institutions may lack the staff and funding for in-house expertise or AI red-teaming or red team/blue team exercises[134] but still need to mitigate against AI risk. Accordingly, small institutions should be required to undergo AI security audits by outside consultants to determine where vulnerabilities lie. These audits help identify and address any vulnerabilities in AI systems

that might be exploited by cyber threats, thus enhancing overall cybersecurity measures. The CFPB may require such audits because failure to do so while claiming accurate and secure systems is unfair. Regulators should set guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.** Requiring nonbank consumer financial service providers to disclose their annual resources dedicated to cybersecurity and AI risk management and compliance is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in financial institution operations,[135] the potential vulnerabilities and risks associated with cyber threats amplify significantly. The CFPB could enact regulations mandating such resource disclosures for spending on cybersecurity and AI risk management and compliance. By mandating such disclosures, stakeholders, including customers, regulators, and investors, would gain valuable insights into the extent of an institution's commitment to mitigating cyber risks through AI.

Federal Deposit Insurance Act, Federal Credit Union Act, and Bank Holding Company Act

Relevant agencies: *Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration*

The Federal Deposit Insurance Act (FDIA) and the Federal Credit Union Act (FCUA) are two of the core statutes that permit banking and credit union regulators to ensure the safety and soundness of institutions under their respective jurisdictions.[136] The Bank Holding Company Act (BHCA) similarly provides the Federal Reserve with many of the same authorities for bank holding companies. Under these statutes, banking regulators are required to prescribe standards relating to "internal controls, information systems, and internal audit systems" as well as any "other operational and managerial standards as the agency determines to be appropriate."[137] The National Credit Union Administration (NCUA) is required to "promulgate rules establishing minimum standards ... of security devices and procedures."[138] Regulators may also enforce prohibitions against activities that are unsafe or unsound.[139]

Pursuant to these authorities, regulators have issued a wide array of regulations and guidance designed to ensure financial institutions adhere to the highest operational standards. For example, they have issued guidelines establishing standards for safety and soundness covering loan documentation, credit underwriting, and asset quality.[140] They have also issued information security standards "for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[141] Regulators

routinely examine institutions to ensure adherence to heightened standards and to identify unsafe or unsound activities and issue a host of guidance identifying risky acts and practices that institutions may consider addressing.[142]

Recommendations

Using these authorities, the Federal Reserve, FDIC, OCC, and NCUA should consider the following actions:

- **Require financial institutions' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict standards and require those institutions to periodically review their customer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems provide customers with accurate information about their accounts, their firms' policies and procedures, and the law. In addition, as these AI systems begin to be used for more than simply providing information – such as executing customers' money transfers or asset purchases – it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and within firms' policies. Regulators must ensure that institutions' customer-facing AI systems are accurate and require periodic reviews of their systems to ensure accuracy.

- **Ensure banks' capital structures can withstand sudden and deep withdrawals of customer deposits or losses from banks' risk management processes.** Banks' corporate clients are likely to begin using AI systems for treasury management – including bank deposits – and there are likely to be only a small number of providers of such systems, given the large computing power necessary for effective AI.[143] AI-based treasury management systems may automatically move all firms' cash, simultaneously creating significant movements of cash between financial institutions in short periods of time that result in sudden and significant drops in customer deposits. Regulators must ensure that banks maintain sufficient shareholder capital and high-quality liquid assets that enable them to withstand such shifts without failing.

- **Require that AI systems that are parts of banks' capital, investment, and other risk management models be explainable.** Banks today use various systems to automate their capital management strategies, evaluate investment opportunities, and otherwise mitigate risk. They will inevitably use AI for these and other purposes that have significant effects on their profitability and stability. The banking agencies already review firms' risk management practices regarding the various models they use, and regulators should do the same with AI. Specifically, all AI systems must be explainable to expert and lay audiences. Examiners must be allowed to review source code and dataset acquisition protocols.

- **Ensure firms may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not develop their own systems in-house; instead, they will license software from a few competing nonfinancial institutions.[144] Financial firms must be able to move between different and competing AI systems to avoid lock-in. Accordingly, regulators should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. Regulators must ensure that there are many – for example, at least five – providers of AI software for banks that provide for base interoperability, so that not all institutions are using the same one or two pieces of software.

- **Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in banking operations, the potential vulnerabilities and risks associated with cyber threats amplify significantly. By mandating such disclosures, stakeholders, including customers, regulators, and investors, gain valuable insights into the extent of a bank's commitment to mitigating cyber risks through AI. Bank and credit union annual disclosures could provide these disclosures.

Dodd-Frank Act: Systemic risk designation

Relevant agency: *Financial Stability Oversight Council*

The Dodd-Frank Act (DFA), enacted following the great financial crisis of 2007–2008, created the Financial Stability Oversight Council to "identify risks to the financial stability of the United States" and "respond to emerging threats to the stability of the United States financial system."[145] Among the authorities the DFA granted to the FSOC is the ability to designate financial market utilities (FMUs) as systemically important and subject to supervision and regulation by the Federal Reserve. Under statute, FMUs are "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person."[146]

To designate FMUs, the FSOC can merely determine that they "are, or are likely to become, systemically important."[147] To make this determination, the FSOC is statutorily required to consider five factors: 1) "the aggregate monetary value of transactions processed by the financial market utility"; 2) "the aggregate exposure of the financial market utility ... to its counterparties"; 3) "the relationship, interdependencies, or other interactions of the financial market utility ... with other financial

market utilities or payment, clearing, or settlement activities"; 4) "the effect that the failure of or a disruption to the financial market utility ... would have on critical markets, financial institutions, or the broader financial system"; and 5) "any other factors that the Council deems appropriate."[148] In the FSOC's rules detailing its process for designating FMUs, it provides that it makes "two critical determinations" in deciding whether to act: first, "whether the failure of or a disruption to the functioning of the FMU now or in the future could create, or increase, the risk of significant liquidity or credit problems spreading among financial institutions or markets"; second, "whether the spread of such liquidity or credit problems among financial institutions or markets could threaten the stability of the financial system of the United States."[149] Using this authority, the FSOC has designated eight FMUs, all clearinghouses.[150]

In a March 2024 interview with Politico, SEC Chair Gary Gensler warned about the dangers of concentration with AI and financial systems: "We have set up a lot of our systems of oversight and rules around regulating individual entities or activities, whether it's bank regulators, insurance regulators, securities regulators, commodities regulators." Gensler added that it was important to be "thinking about [AI] across all the entities — are they potentially all using the same base model or base data?"[151] He also noted the threat of AI concentration in the financial system, saying: "I would be quite surprised if in the next 10 or 20 years a financial crisis happens and there wasn't somewhere in the mix some overreliance on one single data set or single base model somewhere."[152]

While AI usage has yet to reach levels that justify designation as FMUs, if AI has the impact and widespread adoption predicted by some, then that future designation may be warranted.

Recommendations

Using this FMU designation authority, the FSOC should consider the following actions in the event that major providers of AI services reach a level of systemic importance to warrant oversight under these authorities:

- **Designate major providers of AI services to financial institutions as systemically important if they reach an adoption level that creates vulnerability.** It may appear incongruous at first glance to designate AI service providers as not only systemically important but also as systemically important FMUs. They do not facilitate payments, are not clearinghouses, do not provide for settlement of financial transactions, nor do they engage in significant financial transactions with counterparties. However, providers of AI services to the largest and most systemically important financial institutions could still meet the FSOC's two determinations if they become so important to traders and market makers that, if the AI systems stop working for those firms, it "could create, or increase, the risk of significant liquidity or credit problems [in the markets]."[153]

Consider, for example, that market makers such as investment banks use AI systems to facilitate trades. If those systems stop working or execute faulty trades, significant liquidity could be removed from the markets, causing asset prices to drop precipitously along with financial instability. Similar arguments may be made for brokers using AI to manage their funding needs: If AI systems stop working, those brokers could lose access to funding sources, causing them to collapse. And the same is potentially true for high-frequency traders using AI to manage their trades – as faulty AI systems could result in flash crashes. Accordingly, the FSOC should monitor which AI systems are relied on by significant players in the markets and consider designating them as systemically important if their failure could threaten the stability of the U.S. financial system.

- **Designate the cloud service providers to those firms designated as systemically important.** AI systems rely on cloud service providers, such as Amazon Web Services or Microsoft Azure, to operate; thus, if these cloud providers fail, AI systems also fail.[154] Indeed, AI programs run on cloud providers' servers and require cloud providers' computing power to conduct the large-scale language processing required for AI. To the extent that AI software is of systemic importance to the financial system and may pose systemic risks if it fails, the fact that AI software cannot operate without cloud providers means that cloud providers are also of systemic importance to the financial system and may pose systemic risks themselves. This is not a new idea; members of Congress and advocacy organizations have previously called for such designation.[155] However, the rise of AI gives this proposal new urgency. Accordingly, once the FSOC identifies which AI systems are systemically important, it should determine the cloud providers on which they rely and consider designating them as systemically important.

Securities Exchange Act of 1934

Relevant agency: *Securities and Exchange Commission*

The Securities Exchange Act of 1934, or "1934 Act," is a cornerstone of securities regulation in the United States, enacted to ensure transparency, integrity, and fairness within the securities markets.[156] The 1934 Act created the Securities and Exchange Commission to regulate the markets and enacted rules governing the secondary trading of securities. It aims to protect investors by mandating the disclosure of crucial financial information, preventing fraudulent practices such as insider trading and market manipulation, and overseeing the operations of securities exchanges.

The 1934 Act governs, and allows the SEC to regulate, brokers, exchanges and alternative trading systems, and clearinghouses, among other institutions. It broadly enables the SEC "to make such rules and regulations as may be necessary or appropriate to implement [the act]."[157] In addition, the 1934 Act provides the SEC with

authority to enact regulations specific to different market participants or registered entities. For example, Section 15 of the act, permits the SEC to "establish minimum financial responsibility requirements" and "standards of operational capability" for brokers,[158] which it has used to enact net capital requirements,[159] risk management practices,[160] and an array of information technology standards.[161] Furthermore, the combination of sections 6, 11A, 15A, and 17A permits the SEC to "facilitate the establishment of a national market system for securities" by allowing it to enact rules requiring exchanges and clearinghouses to "[have] the capacity to . . . carry out the purposes of [the act]."[162] Under these authorities, the SEC enacted Regulation Systems Compliance and Integrity, a comprehensive information technology regulation that requires these entities to "establish written policies and procedures" that "ensure that their systems have levels of capacity, integrity, resiliency, availability, and security" and "[create] business continuity and disaster recovery plans."[163]

Recommendations

Using these authorities, the SEC should consider the following actions:

- **Require that AI systems that are parts of brokers' capital, investment, and other risk management models be explainable.** Brokers use a variety of systems to automate their capital management strategies, evaluate investment opportunities, and mitigate risk. They will inevitably use AI for these and other purposes that significantly affect their profitability and stability. The SEC already regulates brokers' risk management models,[164] and it should do the same with AI. Specifically, all AI systems must be explainable to expert and lay audiences. The SEC should also ensure that it and FINRA's examiners may review source code and dataset acquisition protocols.

- **Require brokers' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards, with those brokers periodically reviewing their customer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems must provide clients with accurate information about their accounts, their policies and procedures, and the law. In addition, as these AI systems are used for more than simply providing information – such as executing customer trades – it is critical that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and within firms' policies. The SEC must ensure that brokers' customer-facing AI systems undergo periodic review to ensure accuracy through third-party audits.

- **Require brokers using AI systems to make investment recommendations to ensure those systems are explainable and operate in clients' best interests.** There may come a day when AI systems are used to make investment recommendations. Before that occurs, the SEC must make clear that any AI systems used for that purpose must comply with existing rules that require investment recommendations to be in clients' best interests.[165] Among other things, AI systems must be explainable to expert and lay audiences. Brokers must also be able to explain why their recommendations are not provided based on conflicts of interest. Furthermore, the SEC should require brokers using AI to make investment recommendations to periodically review those systems and ensure that examiners may review source code and dataset acquisition protocols.

- **Require red-teaming of AI for exchanges, alternative trading systems, and clearinghouses.** AI red-teaming is defined as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[166] The largest firms should already be utilizing red teaming for their AI products. In addition, they should be running red team/blue team exercises, and the agencies should require the teams to incorporate AI into their efforts. Using AI can significantly increase the speed with which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[167] Firms must be aware of how malicious actors can use AI to attack their infrastructure to be able to defend against it. Banks and other financial institutions must conduct AI red-teaming to fortify their cyber defenses and proactively identify vulnerabilities. Given the systemic importance of these firms, the SEC should not allow third-party audits to suffice, but rather deploy multiple steps to ensure security and protection.

- **Ensure firms may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not develop their own systems in-house; instead, they will license software from a few competing nonfinancial institutions.[168] It will be imperative that financial firms be able to move between different and competing AI systems to avoid lock-in. Accordingly, the SEC should make it a prerequisite of using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. The SEC could require that brokers, exchanges, alternative trading systems, and clearinghouses ensure that there are many—for example, at least five—providers of AI software that provide for base interoperability before entering contracts, so that not all institutions are using the same one or two pieces of software.

- **Require disclosure of annual resources dedicated to cybersecurity spending and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance for transparency and accountability. Given the escalating reliance on AI-driven technologies in financial services, the potential vulnerabilities and risks associated with cyber threats amplify significantly. The SEC should, accordingly, mandate brokers, exchanges, and clearinghouses to disclose their annual expenditures on cybersecurity and AI risk management and compliance. By mandating such disclosures, the SEC can gain valuable insights into the extent of a firm's commitment to mitigating AI risk management.

Investment Advisers Act of 1940

Relevant agency: *Securities and Exchange Commission*

The Investment Advisers Act (IAA) regulates the activities of firms providing investment advice to clients. Under the IAA, investment advisers must register with the Securities and Exchange Commission if they manage assets above certain thresholds, becoming registered investment advisers (RIAs); comply with SEC regulations; and adhere to a fiduciary duty vis-à-vis their clients. Under the IAA, the SEC may regulate how firms safeguard client assets over which they have custody[169] and may "promulgate rules prohibiting or restricting certain sales practices, conflicts of interest, and compensation schemes for brokers, dealers, and investment advisers that the Commission deems contrary to the public interest and the protection of investors."[170]

Recommendations

Accordingly, the SEC should consider the following actions:

- **Require that RIAs' AI systems used to make investment recommendations are explainable and operate in clients' best interests.** There may come a day when AI systems are used to make investment recommendations. Before that occurs, the SEC must make clear that any AI systems used for that purpose must comply with existing rules that require investment recommendations to be in clients' best interests. Among other things, RIAs' AI systems must be explainable to both expert and lay audiences and explain why their recommendations are not provided based on conflicts of interest. Furthermore, the SEC should require RIAs that use AI to make investment recommendations to periodically review those systems and ensure that examiners may review source code and dataset acquisition protocols.

- **Require RIAs' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards, with RIAs periodically reviewing their customer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems provide clients with accurate information about their accounts, their firms' policies and procedures, and the law in a manner that is not misleading. In addition, as these AI systems begin to be used for more than simply providing information – such as executing customer trades – it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only legal transactions within firms' policies. The SEC must ensure that RIAs' customer-facing AI systems are accurate and require periodic reviews of their systems to ensure accuracy.

- **Ensure RIAs may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not be developing their systems in-house; instead, they will license software from a small number of competing nonfinancial institutions.[171] It is imperative that RIAs are able to move between different and competing AI systems to avoid lock-in. Accordingly, the SEC should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. The SEC must require that RIAs ensure that there are many – for example, at least five – providers of AI software that provide for base interoperability before entering contracts, so that not all institutions are using the same one or two pieces of software.

Commodity Exchange Act

Relevant agency: *Commodity Futures Trading Commission*

The Commodity Exchange Act (CEA) regulates the trading of commodity futures and other derivatives to ensure fair and efficient markets while preventing fraud and manipulation. The CEA created the Commodity Futures Trading Commission to oversee these markets, which requires the registration and regulation of various registrants, trading platforms, and clearinghouses. Originally enacted to protect farmers and ranchers in hedging their risks, the CEA now also covers trades worth trillions of dollars of value.

The CEA allows the CFTC to "make and promulgate such rules and regulations as, in the judgment of the Commission, are reasonably necessary to effectuate any of the provisions or to accomplish any of the purposes of [the act]."[172] In addition, the CFTC has specific grants of regulatory authority over different market participants.

For example, the CFTC may "prescribe rules applicable to swap dealers and major swap participants," including rules explicitly related to "business conduct standards" and "minimum capital requirements."[173] For futures commission merchants (FCMs), the CFTC may enact "minimum financial requirements"[174] and regulations governing how these entities handle customer assets.[175] Exchanges must comply with acceptable business practices;[176] "have adequate financial, operational, and managerial resources"; "[create risk management programs] to identify and minimize sources of operational risk"; and "establish and maintain emergency procedures, backup facilities, and a plan for disaster recovery"—and the CFTC may prescribe rules governing all of these activities.[177] Similar requirements apply to clearinghouses, which the CFTC can regulate similarly.[178] With these authorities, the CFTC has enacted various regulations, including the first rules on algorithmic trading.[179] The agency has also recently proposed a rule for cyber and operational resilience.[180]

Recommendations

Using these myriad authorities, the CFTC should consider the following actions:

- **Require AI systems that are parts of futures commission merchants', swap dealers', or major swap participants' capital, investment, or other risk management models to be explainable.** Today, these entities use a variety of systems to automate their capital management strategies, evaluate investment opportunities, and mitigate risk. They will inevitably begin using AI for these and other purposes that significantly affect their profitability and stability. The CFTC should regulate its AI models and ensure that all AI systems are explainable to expert and lay audiences. The CFTC should also ensure that it and the National Futures Association's examiners may review source code and dataset acquisition protocols.

- **Require futures commission merchants' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards.** As institutions begin using AI chatbots to communicate with customers, these systems provide clients with accurate information about their accounts, their firms' policies and procedures, and the law. In addition, as these AI systems begin to be used for more than simply providing information – such as executing customer trades – it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and within firms' policies. The CFTC must ensure that FCMs' customer-facing AI systems are accurate in all respects and require periodic reviews of those systems to ensure accuracy and explainability.

- **Require that FCMs' AI systems used to make investment recommendations be explainable and operate in clients' best interests.** There may come a day when AI systems are used to make investment recommendations. Before that occurs, the CFTC must make clear that any AI systems used for that purpose must comply with existing rules that require investment recommendations to be in clients' best interests. Among other things, AI systems must be explainable to expert and lay audiences and explain why recommendations are not provided based on conflicts of interest. Furthermore, the CFTC should require FCMs using AI to make investment recommendations, to periodically review those systems, and to ensure that examiners can review source code and dataset acquisition protocols.

- **Require red-teaming of AI for swap dealers, exchanges, and clearinghouses.** AI red-teaming is defined as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[181] The largest firms should use red-teaming for their AI products. In addition, they should run red team/blue team exercises and require the teams to incorporate AI into their efforts. Using AI can significantly increase the speed with which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[182] Firms must be aware of how malicious actors can use AI to attack their infrastructure to be able to defend against it. Banks and other financial institutions must conduct AI red-teaming to fortify their cyber defenses and proactively identify vulnerabilities.

- **Require third-party AI audits for all institutions.** All institutions should require AI audits. Larger institutions can bring this practice in-house, depending on the ecosystem that develops around AI audits. However, smaller financial institutions may lack the staff and funding for in-house expertise or AI red-teaming but still need to mitigate against AI risk. Accordingly, small institutions should be required to undergo AI security audits by outside consultants to determine where vulnerabilities lie. These audits help identify and address any vulnerabilities in AI systems that might be exploited by cyber threats, thus enhancing overall cybersecurity measures. Regulators should set out guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Ensure firms can move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not be developing their systems in-house; instead, they will license software from a few competing nonfinancial institutions.[183] It is imperative that financial firms are able to move between different and competing AI systems to avoid lock-in. Accordingly, the CFTC should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for an easy transition to a competing

system upon the contract's expiration. The CFTC must require that all registrants and registered entities ensure that there are many – for example, at least five – providers of AI software that provide for base interoperability before entering contracts, so that not all institutions use the same one or two pieces of software.

- **Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in financial services, the potential vulnerabilities and risks associated with cyber threats amplify significantly. Accordingly, the CFTC should mandate that registrants and registered entities disclose their annual expenditures on cybersecurity and AI risk management and compliance. By mandating such disclosures, the CFTC can gain valuable insights into the extent of a firm's commitment to mitigating AI risks.

Conclusion

The numerous U.S. financial regulators have ample statutory authority to address concerns AI may pose to customers, banks, securities brokers and futures commission merchants, securities and derivatives exchanges, and other market intermediaries. U.S. financial regulators must begin to address these challenges now with their existing authorities and tools to ensure the success and stability of the U.S. financial system in the AI age. GFI and CAP hope this chapter will offer thoughtful options to regulators as they undertake their AI work.

Read the fact sheet

The accompanying fact sheet lists all of the recommendations detailed in this chapter of the report.

Endnotes

1 Office of the Law Revision Counsel, "15 USC 9401(3): Definitions," available at https://uscode.house.gov/view.xhtml?req=(title:15%20section:9401%20edition:prelim) (last accessed May 2024).

2 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," *Federal Register* 88 (210) (2023): 75191–75226, available at https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

3 Shalanda D. Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (Washington: Office of Management and Budget, 2024), available at https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

4 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

5 Ibid., Section 8(a).

6 U.S. Department of Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector" (Washington: 2024), p. 21, available at https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.

7 Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights," available at https://www.whitehouse.gov/ostp/ai-bill-of-rights (last accessed February 2024); National Institute of Standards and Technology, "AI Risk Management Framework," available at https://www.nist.gov/itl/ai-risk-management-framework (last accessed February 2024); Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"; Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

8 Deloitte, "The implications of generative AI in Finance," available at https://www2.deloitte.com/us/en/pages/consulting/articles/generative-ai-in-finance.html (last accessed February 2024).

9 The White House, "Blueprint for an AI Bill of Rights" (Washington: 2022), available at https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

10 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Appendix I, Section 2.k., p. 32.

11 Jared Kaplan and others, "Scaling Laws for Neural Language Models" (2020), available at https://arxiv.org/abs/2001.08361; Andrew J. Lohn and Micah Musser, "AI and Compute: How Much Longer Can Computing Power Drive Artificial Intelligence Progress?" (Washington: Center for Security and Emerging Technology, 2022), available at https://cset.georgetown.edu/publication/ai-and-compute/; Amba Kak and Dr. Sarah Myers West, "2023 Landscape: Executive Summary (Confronting Tech Power)" (New York: AI Now Institute, 2023), available at https://ainowinstitute.org/general/2023-landscape-executive-summary.

12 Cheyenne DeVon, "Scammers can use AI tools to clone the voices of you and your family – how to protect yourself," CNBC, January 24, 2024, available at https://www.cnbc.com/2024/01/24/how-to-protect-yourself-against-ai-voice -cloning-scams.html.

13 Quinn Owen, "How AI can fuel financial scams online, according to industry experts," ABC News, October 11, 2023, available at https://abcnews.go.com/Technology/ai-fuel-financial-scams-online-industry-experts/story?id=103732051.

14 Office of the Comptroller of the Currency, "Suspicious Activity Reports (SAR)," available at https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html (last accessed February 2024).

15 Financial Stability Oversight Council, "Annual Report 2023" (Washington: U.S. Department of the Treasury, 2023), available at https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf.

16 Evan Weinberger, "Bank Regulators Look to Existing Tools to Police AI Advances," Bloomberg Law, July 10, 2023, available at https://news.bloomberglaw.com/banking-law/bank-regulators-look-to-existing-tools-to-police-ai-advances.

17 Michael Akinwumi and others, "An AI fair lending policy agenda for the federal financial regulators" (Washington: Brookings Institution, 2021), available at https://www.brookings.edu/articles/an-ai-fair-lending-policy-agenda-for-the-federal- financial-regulators/.

18 Evan Weinberger, "Banks Warned Against Relying on Error-Prone, Alienating Chatbots," Bloomberg Law, June 6, 2023, available at https://news.bloomberglaw.com/banking-law/banks-use-of-chatbots-poses-risks-for-customers-cfpb-says.

19 Financial Industry Regulatory Authority, "AI Applications in the Securities Industry," available at https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry/ai-apps-in-the-industry (last accessed May 2024).

20 ABA Banking Journal, "Regulators say banks responsible for ensuring AI complies with law," January 19, 2024, available at https://bankingjournal.aba.com/2024/01/regulators-say-banks-responsible-for-ensuring-ai-complies-with-law.

21 Board of Governors of the Federal Reserve System, "The Fed Explained," available at https://www.federalreserve.gov/aboutthefed/the-fed-explained.htm (last accessed February 2024).

22 MIT Technology Review, "Preparing for AI-enabled cyberattacks," April 8, 2021, available at https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/.

23 Many institutional clients may use the same AI systems and withdraw funds from individual institutions en masse, causing runs.

24 Nick Huber, "Is artificial intelligence the right technology for risk management?", *Financial Times*, May 15, 2023, available at https://www.ft.com/content/ca4e6538-00fe-4c75-b664-90b4b4079863.

25 Reena R. Bajowala, "SEC Comment Period on Proposed AI Rules for Broker-Dealers and Investment Advisors Closes Oct. 10, 2023," *The National Law Review*, October 3, 2023, available at https://www.natlawreview.com /article/sec-comment-period-proposed-ai-rules-broker-dealers-and-investment-advisors-closes; U.S. Securities and Exchange Commission, "Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers," *Federal Register* 88 (152) (2023): 53960–54024, available at https://www.federalregister.gov/documents/2023/08/09/2023-16377/conflicts-of-interest-associated-with-the-use-of-predictive-data-analytics-by-broker-dealers-and.

26 Jon Hill, "CFPB's Chopra Warns AI Could Spark Flash Crash, Bank Runs," Law 360, November 30, 2023, available at https://www.law360.com/articles/1771207/cfpb-s-chopra-warns-ai-could-spark-flash-crash-bank-runs?copied=1.

27 David Skeel, "What if a clearinghouse fails?", Brookings Institution, June 6, 2017, available at https://www.brookings.edu/articles/what-if-a-clearinghouse-fails.

28 The White House, "Blueprint for an AI Bill of Rights," p. 8; Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

29 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

30 Ibid.

31 Ibid., Section 8(a).

32 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

33 Consumer Financial Protection Bureau, "Consumer Financial Protection Bureau Strategic Plan: FY 2022 - 2026" (Washington), available at https://files.consumerfinance.gov/f/documents/cfpb_strategic-plan_fy2022-fy2026.pdf (last accessed May 2024).

34 Andrew Carobus, "CFPB Director Chopra addresses AI concerns," Ballard Spahr LLP, December 6, 2023, available at https://www.consumerfinancemonitor.com/2023/12/06/cfpbs-director-chopra-addresses-potential-for-ai-to-give-enormous-power-to-few/.

35 Hill, "CFPB's Chopra Warns AI Could Spark Flash Crash, Bank Runs."

36 Reuters, "US watchdog to announce plans to regulate 'surveillance industry'," August 15, 2024, available at https://www.reuters.com/world/us/us-watchdog-announce-plans-regulate-surveillance-industry-2023-08-15/.

37 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms" (Washington: 2022), available at https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

38 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B" (Washington: 2023), available at https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

39 Consumer Financial Protection Bureau, "Annual report of credit and consumer reporting complaints" (Washington: 2023), available at https://files.consumerfinance.gov/f/documents/cfpb_fcra-611-e_report_2023-01.pdf.

40 Rohit Chopra and others, "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems," Press release, Consumer Financial Protection Bureau and others, April 25, 2023, available at https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

41 Consumer Financial Protection Bureau, "CFPB Orders Wells Fargo to Pay $3.7 Billion for Widespread Mismanagement of Auto Loans, Mortgages, and Deposit Accounts," Press release, December 20, 2022, available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-wells-fargo-to-pay-37-billion-for-widespread-mismanagement-of-auto-loans-mortgages-and-deposit-accounts/.

42 Consumer Financial Protection Bureau, "Enforcement Actions: Hello Digit, LLC," available at https://www.consumerfinance.gov/enforcement/actions/hello-digit-llc/ (last accessed February 2024).

43 Evan Weinberger, "Banks' Reliance on Automated Compliance Systems Draws CFPB's Eyes," Bloomberg Law, January 20, 2023, available at https://news.bloomberglaw.com/banking-law/banks-reliance-on-automated -compliance-systems-draws-cfpbs-eyes.

44 U.S. Department of the Treasury, "Remarks by Assistant Secretary for Financial Institutions Graham Steele at the Amazon Web Services (AWS) Gov2Gov Summit on Responsible Artificial Intelligence Innovation for the Public Sector," Press release, October 24, 2023, available at https://home.treasury.gov/news/press-releases/jy1837.

45 U.S. Department of the Treasury, "READOUT: Deputy Secretary of the Treasury Wally Adeyemo's Meeting with the Financial and Banking Information Infrastructure Committee," Press release, February 2, 2024, available at https://home.treasury.gov/news/press-releases/jy2074.

46 Financial Stability Oversight Council, "Annual Report 2023."

47 Janet Yellen, "Statement by Janet L. Yellen, Secretary, United States Department of the Treasury, before the Committee on Financial Services," U.S. House of Representatives, February 6, 2024, available at https://docs.house.gov/meetings/BA/BA00/20240206/116798/HHRG-118-BA00-Wstate-YellenJ-20240206.pdf.

48 U.S. Department of Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector."

49 Ibid., p. 35.

50 Office of the Comptroller of the Currency, "Acting Comptroller Discusses Tokenization, Artificial Intelligence," Press release, June 16, 2023, available at https://www.occ.gov/news-issuances/news-releases/2023/nr-occ-2023-64.html; Office of the Comptroller of the Currency, "Semiannual Risk Perspective From the National Risk Committee" (Washington: 2023), available at https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-fall-2023.pdf; Board of Governors of the Federal Reserve System and others, "Agencies seek wide range of views on financial institutions' use of artificial intelligence," Press release, March 29, 2021, available at https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210329a.htm.

51 Office of the Comptroller of the Currency, "OCC Establishes Office of Financial Technology," Press release, March 30, 2023, available at https://www.occ.gov/news-issuances/news-releases/2023/nr-occ-2023-31.html.

52 Rajashree Chakravarty, "Republican lawmakers raise concerns over FDITech," Banking Dive, February 5, 2024, available at https://www.bankingdive.com/news/FDIC-fditech-Mchenry-Barr-French-Hill-fintech-innovation-occ/706566/.

53 Board of Governors of the Federal Reserve System, "Other Resources," available at https://www.federalreserve.gov/aboutthefed/innovation-other-resources.htm (last accessed February 2024).

54 Board of Governors of the Federal Reserve System and others, "Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning," *Federal Register* 86 (60) (2021): 16837–16842, available at https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

55 Rohit Chopra, "Algorithms, artificial intelligence, and fairness in home appraisals," Consumer Financial Protection Bureau, June 1, 2023, available at https://www.consumerfinance.gov/about-us/blog/algorithms-artificial-intelligence-fairness-in-home-appraisals/.

56 Andrew Ross Sorkin, and others, "The S.E.C.'s Chief Is Worried About A.I.," *The New York Times*, August 7, 2023, available at https://www.nytimes.com/2023/08/07/business/dealbook/sec-gensler-ai.html.

57 Declan Harty and Steven Overly, "Gensler's warning: Unchecked AI could spark future financial meltdown," Politico, March 19, 2024, available at https://www.politico.com/news/2024/03/19/sec-gensler-artificial-intelligence-00147665.

58 U.S. Securities and Exchange Commission, "Strategic Hub for Innovation and Financial Technology (FinHub)," available at https://www.sec.gov/finhub (last accessed February 2024).

59 U.S. Securities and Exchange Commission, "SEC Proposes New Requirements to Address Risks to Investors From Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers," Press release, July 26, 2023, available at https://www.sec.gov/news/press-release/2023-140.

60 Richard Vanderford, "SEC Probes Investment Advisers' Use of AI," *The Wall Street Journal*, December 10, 2023, available at https://www.wsj.com/articles/sec-probes-investment-advisers-use-of-ai-48485279.

61 U.S. Securities and Exchange Commission, "Investor Bulletin: Robo-Advisers," February 23, 2017, available at https://www.sec.gov/oiea/investor-alerts-bulletins/ib_roboadvisers.

62 U.S. Securities and Exchange Commission, "Observations from Examinations of Advisers that Provide Electronic Investment Advice" (Washington: 2021), available at https://www.sec.gov/files/exams-eia-risk-alert.pdf.

63 Financial Industry Regulatory Authority, "What We Do," available at https://www.finra.org/about/what-we-do (last accessed February 2024).

64 Financial Industry Regulatory Authority, "FinTech," available at https://www.finra.org/rules-guidance/key-topics/fintech (last accessed February 2024).

65 Financial Industry Regulatory Authority, "Artificial Intelligence (AI) in the Securities Industry" (Washington: 2020), available at https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf.

66 Commodity Futures Trading Commission, "A Primer on Artificial Intelligence in Financial Markets" (Washington: 2019), available at https://www.cftc.gov/media/2846/LabCFTC_PrimerArtificialIntelligence102119/download.

67 Commodity Futures Trading Commission, "CFTC Division of Enforcement Creates Two New Task Forces," Press release, June 29, 2023, available at https://www.cftc.gov/PressRoom/PressReleases/8736-23.

68 Commodity Futures Trading Commission, "Commissioner Goldsmith Romero Announces Technology Advisory Committee Meeting Agenda That Includes Cybersecurity, Decentralized Finance, and Artificial Intelligence," Press release, March 22, 2023, available at https://www.cftc.gov/PressRoom/Events/opaeventtac032223.

69 See, for example, Commodity Futures Trading Commission, "Remarks of Commissioner Christy Goldsmith Romero: Financial Stability is Foundational for Consumer Protection," Press release, November 16, 2023, available at https://www.cftc.gov/PressRoom/SpeechesTestimony/oparomero13.

70 National Institute of Standards and Technology, "AI Risk Management Framework"; Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"; Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights"; Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

71 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

72 Inioluwa Deborah Raji and others, "Outsider Oversight: Designing a Third Party Audit Ecosystem for AI Governance" (2022), available at https://www.skillscommons.org/bitstream/handle/taaccct/18870/Raji_et_al_2022_Outsider_Oversight.pdf?sequence=3&isAllowed=y.

73 Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights."

74 The White House, "Notice and Explanation," available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/notice-and-explanation/ (last accessed February 2024).

75 Executive Office of the President, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

76 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," footnote 50, p. 23.

77 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

78 OpenAI, "GPT-4 System Card" (San Francisco: 2023), available at https://cdn.openai.com/papers/gpt-4-system-card.pdf; Ram Shankar and Siva Kumar, "Announcing Microsoft's open automation framework to red team generative AI Systems," Microsoft, February 22, 2024, available at https://www.microsoft.com/en-us/security/blog/2024/02/22/announcing-microsofts-open-automation-framework-to-red-team-generative-ai-systems/; Meta, "Introducing Purple Llama for Safe and Responsible AI Development," December 7, 2023, available at https://about.fb.com/news/2023/12/purple-llama-safe-responsible-ai-development/.

79 Alan Mislove, "Red-Teaming Large Language Models to Identify Novel AI Risks," Office of Science and Technology Policy, August 29, 2023, available at https://www.whitehouse.gov/ostp/news-updates/2023/08/29/red-teaming-large-language-models-to-identify-novel-ai-risks/; The White House, "Voluntary AI Commitments" (Washington: 2023), available at https://www.whitehouse.gov/wp-content/uploads/2023/09/Voluntary-AI-Commitments-September-2023.pdf.

80 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"; Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

81 Laiba Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?", Splunk, May 17, 2023, available at https://www.splunk.com/en_us/blog/learn/red-team-vs-blue-team.html.

82 Aviv Ovadya, "Red Teaming Improved GPT-4. Violet Teaming Goes Even Further," *Wired*, March 29, 2023, available at https://www.wired.com/story/red-teaming-gpt-4-was-valuable-violet-teaming-will-make-it-better/.

83 The White House, "National Cybersecurity Strategy" (Washington: 2023), available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

84 National Institute of Standards and Technology, "AI Risk Management Framework"; Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

85 Legal Information Institute, "12 U.S. Code § 1951(b) - Congressional findings and declaration of purpose," available at https://www.law.cornell.edu/uscode/text/12/1951 (last accessed May 2024).

86 Legal Information Institute, "31 CFR. § 1010.210–230 - Anti-money laundering programs," available at https://www.law.cornell.edu/cfr/text/31/1010.210 (last accessed May 2024); Legal Information Institute, "31 CFR Subpart B — Programs," available at https://www.law.cornell.edu/cfr/text/31/part-1010/subpart-B (last accessed May 2024); Legal Information Institute, "12 CFR Part 21 — Minimum Security Devices and Procedures, Report of Suspicious Activities, and Bank Secrecy Act Compliance Program," available at https://www.law.cornell.edu/cfr/text/12/part-21 (last accessed May 2024); Legal Information Institute, "12 CFR § 208 Subpart F — Miscellaneous Requirements," available at https://www.law.cornell.edu/cfr/text/12/part-208/subpart-F (last accessed May 2024); Legal Information Institute, "12 CFR Part 353 — Suspicious Activity Reports," available at https://www.law.cornell.edu/cfr/text/12/part-353 (last accessed May 2024). Legal Information Institute, "12 CFR Part 21 — Minimum Security Devices and Procedures, Report of Suspicious Activities, and Bank Secrecy Act Compliance Program," available at https://www.law.cornell.edu/cfr/text/12/part-21 (last accessed May 2024); Legal Information Institute, "12 CFR § 208 Subpart F — Miscellaneous Requirements," available at https://www.law.cornell.edu/cfr/text/12/part-208/subpart-F (last accessed May 2024); Legal Information Institute, "12 CFR Part 353 — Suspicious Activity Reports," available at https://www.law.cornell.edu/cfr/text/12/part-353 (last accessed May 2024).

87 Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)," available at https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html (last accessed February 2024).

88 Ibid.

89 Legal Information Institute, "12 U.S. Code § 1958 - Compliance," available at https://www.law.cornell.edu/uscode/text/12/1958 (last accessed May 2024).

90 Legal Information Institute, "15 U.S. Code § 6801 - Protection of nonpublic personal information," available at https://www.law.cornell.edu/uscode/text/15/6801 (last accessed May 2024).

91 Legal Information Institute, "15 U.S. Code § 6802 - Obligations with respect to disclosures of personal information," available at https://www.law.cornell.edu/uscode/text/15/6802 (last accessed May 2024).

92 Legal Information Institute, "15 U.S. Code § 6801."

93 See, for example, Legal Information Institute, "12 CFR Appendix B to Part 364 — Interagency Guidelines Establishing Information Security Standards," available at https://www.law.cornell.edu/cfr/text/12/appendix-B_to_part_364 (last accessed May 2024).

94 See, generally, Federal Deposit Insurance Corporation, "Information Technology (IT) and Cybersecurity," available at https://www.fdic.gov/resources/bankers/information-technology/ (last accessed February 2024).

95 The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

96 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

97 Legal Information Institute, "15 U.S. Code § 1691 - Scope of prohibition," available at https://www.law.cornell.edu/uscode/text/15/1691 (last accessed May 2024).

98 Legal Information Institute, "15 U.S. Code § 1691b - Promulgation of regulations by the Bureau," available at https://www.law.cornell.edu/uscode/text/15/1691b (last accessed May 2024).

99 Legal Information Institute, "15 U.S. Code § 1691."

100 Christine Polek and Shastri Sandy, "The Disparate Impact of Artificial Intelligence and Machine Learning," *Colorado Technology Law Journal* 21 (1) (2023): 85–108, available at https://ctlj.colorado.edu/wp-content/uploads/2023/08/FINAL-3-SP-6.17.23_AK-edits-3.pdf.

101 Consumer Financial Protection Bureau, "CFPB Consumer Laws and Regulations" (Washington: 2013), available at https://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_ecoa-combined-june-2013.pdf.

102 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms."

103 Giorgio Baldassarri Hoger von Hogersthal, "Artificial Intelligence and Alternative Data in Credit Scoring and Credit Risk Surveillance," S&P Global, October 10, 2023, available at https://www.spglobal.com/en/research-insights/featured/special-editorial/artificial-intelligence-and-alternative-data-in-credit-scoring-and-credit-risk-surveillance; Sally Ward-Foxton, "Reducing Bias in AI Models for Credit and Loan Decisions," EE Times, April 30, 2019, available at https://www.eetimes.com/reducing-bias-in-ai-models-for-credit-and-loan-decisions/; Louis DeNicola, "Which Credit Scores Do Mortgage Lenders Use?", Experian, April 22, 2024, available at https://www.experian.com/blogs/ask-experian/which-credit-scores-do-mortgage-lenders-use/; Datrics, "AI Credit Scoring: The Future of Credit Risk Assessment," available at https://www.datrics.ai/articles/the-essentials-of-ai-based-credit-scoring (last accessed March 2024).

104 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 10.1(b)(i).

105 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

106 Legal Information Institute, "15 U.S. Code § 1681 - Congressional findings and statement of purpose," available at https://www.law.cornell.edu/uscode/text/15/1681 (last accessed May 2024).

107 Legal Information Institute, "15 U.S. Code § 1681s–2 - Responsibilities of furnishers of information to consumer reporting agencies," available at https://www.law.cornell.edu/uscode/text/15/1681s-2 (last accessed May 2024).

108 Legal Information Institute, "15 U.S. Code § 1681c - Requirements relating to information contained in consumer reports," available at https://www.law.cornell.edu/uscode/text/15/1681c (last accessed May 2024).

109 Legal Information Institute, "15 U.S. Code § 1681m - Requirements on users of consumer reports," available at https://www.law.cornell.edu/uscode/text/15/1681m (last accessed May 2024).

110 Legal Information Institute, "15 U.S. Code § 1681i - Procedure in case of disputed accuracy U.S. Code," available at https://www.law.cornell.edu/uscode/text/15/1681i (last accessed May 2024).

111 Legal Information Institute, "15 U.S. Code § 1681s - Administrative enforcement," available at https://www.law.cornell.edu/uscode/text/15/1681s (last accessed May 2024).

112 Consumer Financial Protection Bureau, "12 CFR Part 1022.1 Purpose, scope, and model forms and disclosures," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/1/ (last accessed May 2024).

113 Consumer Financial Protection Bureau, "12 CFR Part 1022.42 Reasonable policies and procedures concerning the accuracy and integrity of furnished information," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/42/ (last accessed May 2024).

114 Consumer Financial Protection Bureau, "12 CFR Part 1022.72 General requirements for risk-based pricing notices," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/72/ (last accessed May 2024).

115 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B."

116 *Johnson v. MBNA America Bank, N.A.*, U.S. Court of Appeals for the 4th Circuit, 357 F.3d 426, 432 (February 11, 2004), available at https://casetext.com/case/johnson-v-mbna-america-bank-na (explaining that reasonableness for both kinds of investigations is determined by "weighing the cost of verifying disputed information against the possible harm to the consumer").

117 Legal Information Institute, "15 U.S. Code § 1681a(d)(1) - Definitions; rules of construction," available at https://www.law.cornell.edu/uscode/text/15/1681a#h (last accessed May 2024).

118 Legal Information Institute, "15 U.S. Code § 1681a."

119 Consumer Financial Protection Bureau, "List of Consumer Reporting Companies" (Washington: 2023), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf.

120 Consumer Financial Protection Bureau, "Appendix K to Part 1022 - Summary of Consumer Rights," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/k/ (last accessed February 2024).

121 Consumer Financial Protection Bureau, "Appendix E to Part 1022 - Interagency Guidelines Concerning the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/e/ (last accessed May 2024)

122 Office of the Comptroller of the Currency, "Community Developments Fact Sheet: Community Reinvestment Act" (Washington: 2014), available at https://www.occ.gov/publications-and-resources/publications/community-affairs/community-developments-fact-sheets/pub-fact-sheet-cra-reinvestment-act-mar-2014.pdf.

123 Board of Governors of the Federal Reserve System, "Evaluating a Bank's CRA Performance," available at https://www.federalreserve.gov/consumerscommunities/cra_peratings.htm (last accessed February 2024).

124 Legal Information Institute, "12 U.S. Code § 2905 - Regulations," available at https://www.law.cornell.edu/uscode/text/12/2905 (last accessed May 2024).

125 Legal Information Institute, "12 CFR § 25.27 - Strategic plan," available at https://www.law.cornell.edu/cfr/text/12/25.27 (last accessed May 2024).

126 Office of the Comptroller of the Currency, "12 C.F.R. § 25.41- Community Reinvestment Act (CRA) and Interstate Deposit Production Regulations," available at https://www.occ.gov/topics/consumers-and-communities/cra/12-cfr-part-25.html#:~:text=%C2%A7%2025.41%20Assessment%20area%20delineation.&text=A%20bank%20shall%20delineate%20one,credit%20needs%20of%20its%20community (last accessed May 2024).

127 Legal Information Institute, "Dodd-Frank: Title X - Bureau of Consumer Financial Protection," available at https://www.law.cornell.edu/wex/dodd-frank_title_X (last accessed May 2024).

128 Legal Information Institute, "12 U.S. Code § 5531- Prohibiting unfair, deceptive, or abusive acts or practices," available at https://www.law.cornell.edu/uscode/text/12/5531 (last accessed May 2024).

129 Ibid.

130 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information" (Washington: 2022), available at https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

131 Consumer Financial Protection Bureau, "CFPB and Federal Partners Confirm Automated Systems and Advanced Technology Not an Excuse for Lawbreaking Behavior," Press release, April 25, 2023, available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-federal-partners-confirm-automated-systems-advanced-technology-not-an-excuse-for-lawbreaking-behavior/.

132 The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

133 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

134 NIST Computer Security Resource Center, "Red Team/Blue Team Approach," available at https://csrc.nist.gov/glossary/term/red_team_blue_team_approach (last accessed May 2024).

135 Simon Toms and others, "How Regulators Worldwide Are Addressing the Adoption of AI in Financial Services," Skadden, December 12, 2023, available at https://www.skadden.com/insights/publications/2023/12/how-regulators-worldwide-are-addressing-the-adoption-of-ai-in-financial-services; Board of Governors of the Federal Reserve System and others, "Agencies seek wide range of views on financial institutions' use of artificial intelligence."

136 Federal Deposit Insurance Corporation, "1000 - Federal Deposit Insurance Act," available at https://www.fdic.gov/regulations/laws/rules/1000-100.html (last accessed March 2024); Office of the Law Revision Counsel, "12 USC Ch. 14: Federal Credit Union Act," available at https://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter14&edition=prelim (last accessed March 2024).

137 Legal Information Institute, "12 U.S. Code § 1831p–1 - Standards for safety and soundness," available at https://www.law.cornell.edu/uscode/text/12/1831p-1 (last accessed May 2024); Bank Holding Companies, "12 U.S. Code § 1844 - Administration," available at https://www.law.cornell.edu/uscode/text/12/1844 (last accessed May 2024).

138 Legal Information Institute, "12 U.S. Code § 1785 - Requirements governing insured credit unions," available at https://www.law.cornell.edu/uscode/text/12/1785 (last accessed May 2024).

139 Legal Information Institute, "12 U.S. Code § 1818 - Termination of status as insured depository institution," available at https://www.law.cornell.edu/uscode/text/12/1818 (last accessed May 2024).

140 Legal Information Institute, "12 CFR Appendix A to Part 364 – Interagency Guidelines Establishing Standards for Safety and Soundness," available at https://www.law.cornell.edu/cfr/text/12/appendix-A_to_part_364 (last accessed May 2024).

141 Legal Information Institute, "12 CFR Appendix B to Part 364 – Interagency Guidelines Establishing Information Security Standards," available at https://www.law.cornell.edu/cfr/text/12/appendix-B_to_part_364 (last accessed May 2024); Legal Information Institute, "12 CFR Appendix A to Part 748 – Guidelines for Safeguarding Member Information," available at https://www.law.cornell.edu/cfr/text/12/appendix-A_to_part_748 (last accessed May 2024).

142 See, for example, Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information."

143 U.S. Bank, "How AI in treasury management is transforming finance," May 19, 2023, available at https://www.usbank.com/financialiq/improve-your-operations/manage-payments/ai-thinks-treasury-management-is-ready-for-transformation.html.

144 Miriam Fernández, "AI in Banking: AI Will Be An Incremental Game Changer," S&P Global, October 31, 2023, available at https://www.spglobal.com/en/research-insights/featured/special-editorial/ai-in-banking-ai-will-be-an-incremental-game-changer.

145 Legal Information Institute, "12 U.S. Code § 5322 - Council authority," available at https://www.law.cornell.edu/uscode/text/12/5322 (last accessed May 2024).

146 Legal Information Institute, "12 U.S. Code § 5462 - Definitions," available at https://www.law.cornell.edu/uscode/text/12/5462#6_A (last accessed May 2024).

147 Legal Information Institute, "12 U.S. Code § 5463 - Designation of systemic importance," available at https://www.law.cornell.edu/uscode/text/12/5463 (last accessed May 2024).

148 Ibid.

149 Financial Stability Oversight Council, "Authority To Designate Financial Market Utilities as Systemically Important," *Federal Register* 76 (144) (2011): 44763–44776, available at https://home.treasury.gov/system/files/261/Final-Rule-on-Authority-to-Designate-Financial-Market-Utilities-as-Systemically-Important.pdf.

150 U.S. Department of the Treasury, "Designations," available at https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations (last accessed February 2024).

151 Harty and Overly, "Gensler's warning: Unchecked AI could spark future financial meltdown."

152 Ibid.

153 Legal Information Institute, "Definition: systemic importance from 12 USC § 5462(9)," available at https://www.law.cornell.edu/definitions/uscode.php?height=800&def_id=12-USC-1184801643-149939311&term_occur=999&term_src=title:12:chapter:53:subchapter:IV:section:5463 (last accessed February 2024).

154 Emil Sayegh, "Artificial Intelligence and Clouds: A Complex Relationship of Collaboration and Concern," *Forbes*, August 23, 2023, available at https://www.forbes.com/sites/emilsayegh/2023/08/23/artificial-intelligence-and-clouds-a-complex-relationship-of-collaboration-and-concern/?sh=217106475c19.

155 Pete Schroeder, "U.S. House lawmakers ask regulators to scrutinize bank cloud providers," Reuters, August 23, 2019, available at https://www.reuters.com/article/us-usa-congress-cloud-idUSKCN1VD0Y4/; Action Center on Race & the Economy and others, "Letter to Members of the Financial Stability Oversight Council," November 23, 2021, available at https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/619ce27890a0062ae7014dfd/1637671544609/Designate+AWS+as+a+Systemically+Important+Financial+Market+Utility.pdf.

156 Securities and Exchange Act of 1934, Public Law 291, 73rd Cong., 2nd sess. (June 6, 1934), 15 U.S.C. § 78 et seq., available at https://www.law.cornell.edu/wex/securities_exchange_act_of_1934#:~:text=The%20Securities%20Exchange%20Act%20requires,gain%20control%20of%20the%20company.

157 Legal Information Institute, "15 U.S. Code § 78w - Rules, regulations, and orders; annual reports," available at https://www.law.cornell.edu/uscode/text/15/78w (last accessed May 2024).

158 Legal Information Institute, "15 U.S. Code § 78o - Registration and regulation of brokers and dealers," available at https://www.law.cornell.edu/uscode/text/15/78o (last accessed May 2024).

159 Legal Information Institute, "17 CFR § 240.15c3-1 - Net capital requirements for brokers or dealers," available at https://www.law.cornell.edu/cfr/text/17/240.15c3-1 (last accessed May 2024).

160 Legal Information Institute, "17 CFR § 240.15c3-5 - Risk management controls for brokers or dealers with market access," available at https://www.law.cornell.edu/cfr/text/17/240.15c3-5 (last accessed May 2024); Legal Information Institute, "17 CFR § 240.17h-2T - Risk assessment reporting requirements for brokers and dealers," available at https://www.law.cornell.edu/cfr/text/17/240.17h-2T (last accessed May 2024).

161 Legal Information Institute, "17 CFR § 240.17Ad-12 - Safeguarding of funds and securities," available at https://www.law.cornell.edu/cfr/text/17/240.17Ad-12 (last accessed May 2024).

162 U.S. Securities and Exchange Commission, "Regulation Systems Compliance and Integrity," *Federal Register* 79 (234) (2014): 72251–72447, available at https://www.federalregister.gov/documents/2014/12/05/2014-27767/regulation-systems-compliance-and-integrity#citation-7-p72253.

163 Ibid.

164 Legal Information Institute, "17 CFR § 240.15c3-1e - Deductions for market and credit risk for certain brokers or dealers (Appendix E to 17 CFR 240.15c3-1)," available at https://www.law.cornell.edu/cfr/text/17/240.15c3-1e (last accessed May 2024).

165 Jay Clayton, "Regulation Best Interest and the Investment Adviser Fiduciary Duty: Two Strong Standards that Protect and Provide Choice for Main Street Investors," U.S. Securities and Exchange Commission, July 8, 2019, available at https://www.sec.gov/news/speech/clayton-regulation-best-interest-investment-adviser-fiduciary-duty.

166 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

167 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

168 Mohar Chatterjee, "AI might have already set the stage for the next tech monopoly," Politico March 22, 2023, available at https://www.politico.com/newsletters/digital-future-daily/2023/03/22/ai-might-have-already-set-the-stage-for-the-next-tech-monopoly-00088382.

169 Legal Information Institute, "15 U.S. Code § 80b–18b - Custody of client accounts," available at https://www.law.cornell.edu/uscode/text/15/80b-18b (last accessed May 2024).

170 Legal Information Institute, "15 U.S. Code § 80b–11 - Rules, regulations, and orders of Commission," available at https://www.law.cornell.edu/uscode/text/15/80b-11 (last accessed May 2024).

171 Chatterjee, "AI might have already set the stage for the next tech monopoly."

172 Legal Information Institute, "7 U.S. Code § 12a - Registration of commodity dealers and associated persons; regulation of registered entities," available at https://www.law.cornell.edu/uscode/text/7/12a (last accessed May 2024).

173 Legal Information Institute, "7 U.S. Code § 6s - Registration and regulation of swap dealers and major swap participants," available at https://www.law.cornell.edu/uscode/text/7/6s (last accessed May 2024).

174 Legal Information Institute, "7 U.S. Code § 6f - Registration and financial requirements; risk assessment," available at https://www.law.cornell.edu/uscode/text/7/6f (last accessed May 2024).

175 Legal Information Institute, "7 U.S. Code § 6d - - Dealing by unregistered futures commission merchants or introducing brokers prohibited; duties in handling customer receipts; conflict-of-interest systems and procedures; Chief Compliance Officer; rules to avoid duplicative regulations; swap requirements; portfolio margining accounts," available at https://www.law.cornell.edu/uscode/text/7/6d (last accessed May 2024).

176 Legal Information Institute, "7 U.S. Code § 7a–2 - Common provisions applicable to registered entities," available at https://www.law.cornell.edu/uscode/text/7/7a-2 (last accessed May 2024).

177 Legal Information Institute, "7 U.S. Code § 7b-3 - Swap execution facilities," available at https://www.law.cornell.edu/uscode/text/7/7b-3 (last accessed May 2024); Legal Information Institute, "7 U.S. Code § 7 - Designation of boards of trade as contract markets," available at https://www.law.cornell.edu/uscode/text/7/7 (last accessed May 2024).

178 Legal Information Institute, "7 U.S. Code § 7a–1 - Repealed. Pub. L. 111–203, title VII, § 734(a), July 21, 2010, 124 Stat. 1718," available at https://www.law.cornell.edu/uscode/text/7/7a-1 (last accessed May 2024).

179 Commodity Futures Trading Commission, "Electronic Trading Risk Principles," *Federal Register* 86 (6) (2021): 2048–2077, available at https://www.federalregister.gov/documents/2021/01/11/2020-27622/electronic-trading-risk-principles.

180 Commodity Futures Trading Commission, "CFTC to Hold a Commission Open Meeting on December 13," Press release, December 13, 2023, available at https://www.cftc.gov/PressRoom/Events/opaeventopenmeeting121323.

181 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

182 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

183 Chatterjee, "AI might have already set the stage for the next tech monopoly."