FACT SHEET

Recommendations for Financial Regulatory Agencies To Take Further Action on AI

By Todd Phillips and Adam Conner

This fact sheet collects the recommendations from Chapter 5: "Financial Regulatory Agencies" of the joint report from Governing for Impact (GFI) and the Center for American Progress, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence." The chapter notes how 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 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 using numerous existing authorities. The goal of these recommendations is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. This menu of potential recommendations demonstrates that there are more options for agencies to explore beyond their current work, and that agencies should immediately utilize existing authorities to address AI.

Read the full report

Taking Further Agency Action on AI

Read the full chapter

Financial Regulatory Agencies

In this fact sheet, 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 fact sheet, these agencies include the Treasury Department, the Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation (FDIC); the Commodity Futures Trading Commission (CFTC); the National Credit Union Administration (NCUA); the Securities and Exchange Commission (SEC); the Consumer Financial Protection Bureau (CFPB); the Financial Stability Oversight Council (FSOC), which is chaired by the secretary of the treasury; and, to some extent, the Financial Industry Regulatory Authority (FINRA), the self-regulatory organization for securities brokers, which is overseen by the SEC. It should be noted that other federal agencies not listed here also have financial regulation responsibilities and authorities that could potentially be used to address AI.

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*

Using this authority, 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 Bank Secrecy Act (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 the Financial Crimes Enforcement Network'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*

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 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."[1] 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.[2] 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*

Using this authority, 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,[3] which is a violation of the Equal Credit Opportunity Act (ECOA).[4] 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."[5] 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.[6] 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),[7] whose duties were further outlined in the OMB M-24-10 AI guidance.[8] 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*

As it relates to AI, the CFPB should consider using this authority 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,[9] 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 the 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.[10] 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 Fair Credit Reporting Act (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."[11] "Employment purposes" include the "purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee."[12] 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[13] and issue supervisory guidance explaining the circumstances under which ESAM companies act as credit reporting agencies 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 credit reporting agencies, the CFPB must also make clear that users of their software comply with the FCRA. Accordingly, the CFPB should consider modifying its "Summary of Consumer Rights" to include information about employee FCRA rights concerning employers' use of ESAM technologies.[14] 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.[15]

Community Reinvestment Act

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

The federal banking regulators should consider using their authority to:

- **Require banks to indicate whether they use AI to comply with Community Reinvestment Act (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*

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 unfair, deceptive, or abusive acts or practices (UDAAP) authority can be used to prohibit the inadvertent disclosure of consumers' information at institutions not subject to the Gramm-Leach-Bliley Act.[16] Nonbank consumer financial service providers hold a wealth of information about customers off of which malicious AI systems feed, and they may be liable for customer losses stemming from AI-enabled fraud.[17] With AI red-teaming[18] 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.[19] 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[20] but still need to mitigate 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,[21] 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*

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.[22] 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.[23] 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*

Using its financial market utilities (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]."[24]

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.[25] 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.[26] 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*

Using this authority, 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,[27] 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.[28] 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."[29] 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.[30] 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.[31]

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*

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

- **Require that registered investment advisers' (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.[32] 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*

Using myriad authorities under the Commodity Exchange Act, 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 futures commission merchants' 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."[33] 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.[34] 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.[35] 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.

Endnotes

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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/.

[6] 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).

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

[8] 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.

[9] 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/.

[10] 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”).

[11] 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).

[12] Legal Information Institute, “15 U.S. Code § 1681a.”

[13] 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.

[14] 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).

[15] 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)

[16] 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/.

[17] 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/.

[18] Executive Office of the President, “Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”

[19] Siddiqui, “Red Teams vs. Blue Teams: What’s The Difference?”

[20] 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).

[21] 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.”

[22] 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.

[23] 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.

[24] 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).

[25] 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.

[26] 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.

[27] 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).

[28] 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.

[29] Executive Office of the President, “Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”

[30] Siddiqui, “Red Teams vs. Blue Teams: What’s The Difference?”

[31] 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.

[32] Ibid.

[33] Executive Office of the President, “Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”

[34] Siddiqui, “Red Teams vs. Blue Teams: What’s The Difference?”

[35] Chatterjee, “AI might have already set the stage for the next tech monopoly.”