NELSON MULLINS

Regulation of the Use of AI by Financial Institutions

Richard B. Levin, Kevin Tran, and Bobby Wenner

July 9, 2024

Agenda

- Introduction
- What is AI?
- Definitions
- How will we use AI?
- Example of the Use of AI
- Big Data
- The Explosive Growth of the Use of AI
- Regulatory Considerations
- HAL Meets the Regulators – FTC, SEC, CFTC, and OCC
- Innovations in Compliance

HAL - What is AI

- When regulators and some scholars think of the interactions between humans and AI, some still fear HAL and other forms of AI portrayed in movies.
- The reality is that AI is coming to many industries, including the financial services industry.
- The growth of AI presents a real opportunity to revolutionize the financial services industry, creating efficiencies and reducing costs.

Artificial Intelligence can be thought of broadly as any technology able to perform tasks that would typically require "human thought." This can be anything: (a) understanding something that is seen, (b) recognizing speech, (c) making data-driven decisions, (d) translating among languages, and (e) understanding risks of decisions.

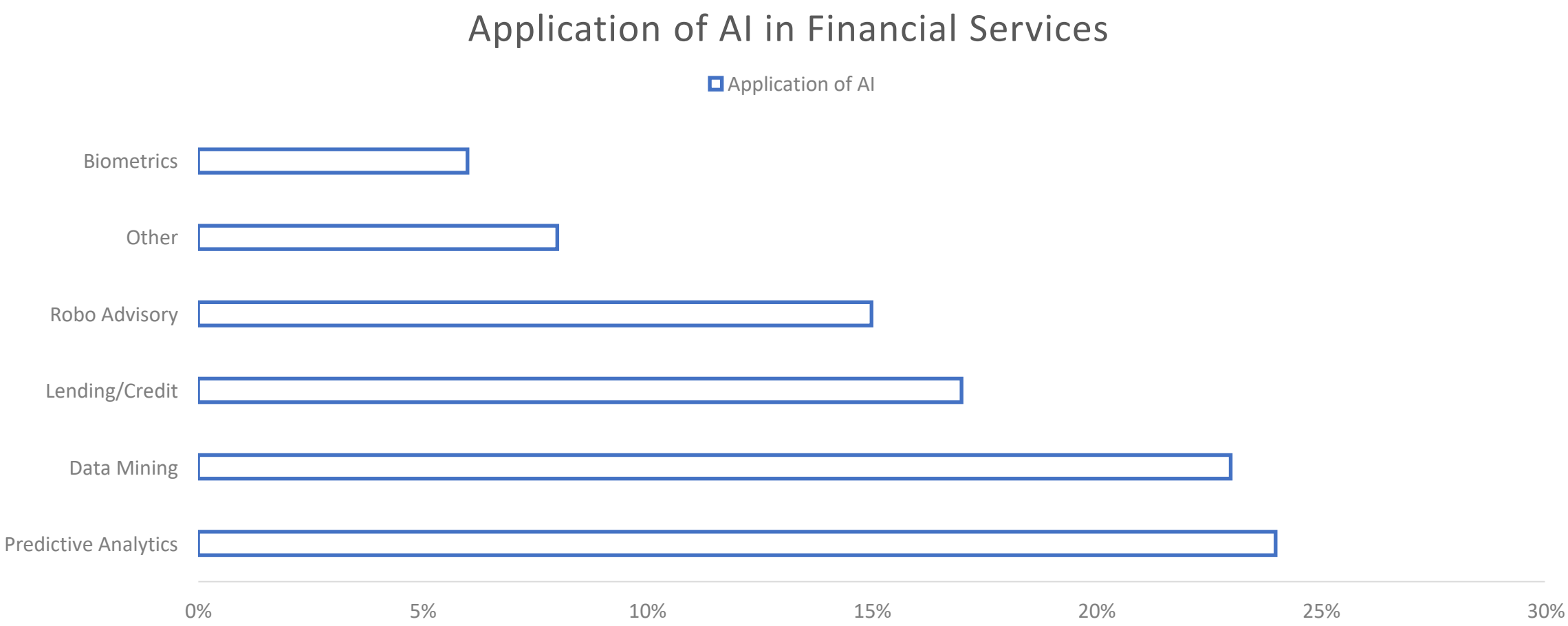
Artificial Intelligence ("AI") encompasses two core concepts: (a) rule-based systems or (b) machine learning ("ML").

Financial services companies are already seeing AI enter the financial services sector. Each year, more FinTech firms are using AI to change how consumers view their relationship with financial services. Now, more than ever, customers expect easier, faster, 24-hour access to financial services.

Definitions

- **Rules-Based Systems**: AI built on a set of algorithms that are used to store, manipulate, and interpret some set of data.
- **Machine Learning**: A set of algorithms to make a system "artificially intelligent"— enabling the system to recognize patterns from large data sets and apply past experiences to predict future results.
- **Natural Language Technologies**: Understanding and interacting with technology as though it were another human—using human language through "Bots" or other natural language generators.
- **Cognitive Data Mapping**: A system that can review data to "understand" what the data means in the way a human would interpret data.
- **Predictive Analytics**: Combines data, statistical algorithms, and machine learning techniques to identify the likelihood of a future outcome based on historical data sets.

How Will We Use AI?



*Goodwin, *A Global Survey of on the State of Financial Technology*

Example of the Use of AI

Analytics-Based Personalization
- Bank's data shows Brad preparing for a trip
- Kevin's mobile banking app offers a customized, 5% personal loan for travel

Bank Sees that Kevin Only Viewed Offer for One Second and Close
- Bank's mobile app offers Kevin a travel rewards credit card with built-in trip protection

Kevin Clicks through to See the Offer
- Kevin chooses to apply
- Instant underwriting looks at Kevin's past loan payments, spending, and deposit activity
- Instant credit decision reached

Kevin Approved for Card
- Kevin is placed in a queue for a call from a banker about fraud protection while traveling
- Kevin's accounts are flagged for overseas travel
- Kevin's debit card is automatically enabled for overseas use

Bank Offers AutoPay Enrollment
- Kevin is presented with an immediate offer to enroll his card in automatic debits —he skips
- Bank waits until the next day and now offers Kevin an incentive to enroll in automatic debits — he accepts

Bank Begins Fraud Monitoring
- Bank's fraud monitoring system refines its red flags to recognize expected overseas travel
- Bank's fraud department successfully intercepts an attempted debit card transaction at a local ATM while Kevin is traveling

Bank Monitors Kevin's Spending on Card
- As Kevin uses card, the Bank's system begins to recognize his spending habits
- Sees he has younger sons
- Begins offering Kevin child savings accounts through mobile banking

Bank's User Profile: **Kevin Tran** (Age 40)

Family: Wife and young sons

Occupation: Working Professional

Other Relationships: Car Loan from Ford Motor Credit

Spending: Entertainment and Travel

Other Financial Products: Brokerage account, AmEx, 529

Profit to Bank: $210/year based on deposit revenue

Big Data

- With the growth of personal computing and the internet, we have seen a dramatic rise in the data generated by the public ("Big Data").
- Big Data has spurred the development of new analytical models that use the data.
- While Big Data has been used by a variety of industries, the financial services industry was an early adopter of the use of the data.
- Early applications of Big Data have included electronic brokerage, high-frequency trading and algorithmic trading.
- The growth of Big Data and the development of machine learning have fueled the use of AI in the financial services industry.
- The development of AI also presents new challenges and opportunities for traditional financial services firms, including exchanges, broker-dealers, investment advisers and banks.
- The growth of trading volumes on alternative trading systems in the late 1990s, and the development of high-frequency trading in the early 21st century, have changed the way securities are traded around the world.
- Today, the majority of the trading of equities listed on the Nasdaq and the NYSE takes place in electronic exchanges.

The Explosive Growth of AI

Reporting, Compliance, & Operations:

- Auto clearing of false sanction screening hits generated by filtering software
- Auto booking of transactions and accounting entries on basis of unstructured data (voice log transcriptions, emails, forms…)
- Automatic reporting
- Increased sophistication of data analysis to better quantify risk
- Third-party vendor oversight and risk management
- Collections management

KYC & Data Protection:

- Big data analysis across systems to generate fraud alerts
- Suitability analysis for customers
- Automatic second line oversight of business units
- KYC reviews, including automatic screening
- Review of communications for possible data leaks
- Review of customer service interactions for prohibited conduct

Marketing & Sales:

- Targeted advertising for individual customers
- Customized product offers
- Real-time analysis of marketing effort ROI
- Real-time customer profitability analysis
- Customer prioritization
- Competitor usage analysis

Client Experience:

- Client satisfaction assessments
- Real-time client behavior patterns
- Real-time product recommendations
- Assessment of client “happiness” during bank interactions
- Early Warning Systems (EWS) for client dissatisfaction
- EWS for loan default
- Lower “marketing fatigue”

Predictive:

- Machine learning based underwriting
- Real time feedback on product design
- Missing solutions analysis
- Bigger data sets feeding customer risks assessments
- Cross-platform and inter-bank data ingestion
- Limit assessments

Regulatory Considerations

Explainability: Without insight into an approach's general operating principles, bank management may not be able to evaluate with confidence how the system will function in unforeseen circumstances.

Data Integrity: Like other systems, AI is designed to interact directly with training data to identify correlations and patterns and use that information for prediction or categorization. If the training data are biased or incomplete, AI may incorporate those shortcomings into its predictions or categorizations.

Overfitting: "Overfitting" can occur when an algorithm "learns" from idiosyncratic patterns in the training data that are not representative of the population as a whole.

Cybersecurity Risks: AI may be exposed to risk from a variety of criminal cybersecurity threats. For example, AI can be vulnerable to "data poisoning attacks," which attempt to corrupt and contaminate training data to compromise the system's performance.

Dynamic Updating: Some AI has the ability to learn or evolve over time, especially as it captures new training data. This can cause drift as it learns from the new data. This can present challenges for validating, monitoring, tracking, and documenting the AI approach, including for persons conducting an independent review.

Third-Party Oversight: Given significant data exchange, TPRM programs are significantly more critical.

Fair Lending/Discrimination/UDAAP: Significant concerns have been raised with "black box" underwriting. There may be uncertainty about how less transparent and explainable AI approaches align with applicable consumer protection legal and regulatory frameworks, which often address fairness and transparency.

Regulatory Questions That Must be Considered

- Is the source data legally obtained?
- Is the source data accurate?
- Are the sources the type that provides FCRA-level data or data actionable by a financial services company?
- Is the reporting agency complying with the FCRA and the FACT Act?
- Is the information being used in compliance with Fair Lending and UDAAP obligations?
- Is the data and its predictive results defensible/predictive?
- How will the company provide proper authorizations and obtain consent from consumers?
- How will the lender disclose adverse actions taken based on the data?
- How can a customer “fix” their standing with the company or improve the risk analysis?

FTC Guidance

- Be truthful about the claims the company can make through its use of AI software.
- Be truthful about the data the company uses.
- Be transparent about how AI software is used and what decisions are made using it.
- Take measures to establish oversight protocols for the use of AI software and its resulting outputs.
- Understand what data sets power the AI model to ensure it would not yield unfair or inequitable results to legally protected groups.

- Michael Atleson, *Keep your AI claims in check*, FTC (Feb. 27, 2023), https://www.ftc.gov/businessguidance/blog/2023/02/keep-your-ai-claims-check
- Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC (Apr. 19, 2021), https://www.ftc.gov/businessguidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai
- Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC (Apr. 9, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms

HAL Meets the Regulators

- The guidance followed the SEC Office of Compliance Inspection and Examinations' priorities letter in January 2017, that identified electronic investment advice as an area of focus for 2017, and the 2016 FinTech Forum, where the growth of robo-advisers was discussed in depth.

- The SEC's guidance included a series of recommendations for robo-advisers to help them meet the disclosure, suitability and compliance obligations under the Investment Advisers Act of 1940 ("Advisers Act").

- The guidance consisted of both elevated level as well as more specific recommendations to help ensure compliance in these areas. The SEC guidance focused on retail robo-advisers that provide their services to clients over the internet.

HAL Meets the Regulators

- The SEC appears ready to abandon this approach to the regulation of the use of AI by investment advisers and broker-dealers.
- In the fall of 2023, the SEC proposed rules with respect to the use of AI that have been widely criticized by the industry and only garnered support from organizations that routinely support the SEC's approach to protecting the public while disregarding one of the other duties of the SEC – promoting capital formation.
- In stark contrast to the SEC's expansive approach to the regulation of AI, earlier this year the U.S. Commodity Futures Trading Commission ("CFTC") published a more measured Request for Comments ("RFC") on a variety of issues related to the use of AI.
- Similarly, the Office of the Comptroller of the Currency ("OCC") has provided guidance that establishes an approach that banks should follow as they look to implement AI.
- SEC Proposed Rule: 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 (July 26, 2023), 88 Fed. Reg. 53,960 (Aug. 9, 2023), available at: https://www.govinfo.gov/content/pkg/FR-2023-08-09/pdf/2023-16377.pdf.

SEC Proposed Rules

- Gensler stated:

  "Today's predictive data analytics models provide an increasing ability to make predictions about each of us as individuals. This raises possibilities that conflicts may arise to the extent that advisers or brokers are optimizing to place their interests ahead of their investors' interests. When offering advice or recommendations, firms are obligated to eliminate or otherwise address any conflicts of interest and not put their own interests ahead of their investors' interests. I believe that, if adopted, these rules would help protect investors from conflicts of interest — and require that, regardless of the technology used, firms meet their obligations not to place their own interests ahead of investors' interests."

- In recent years, financial services firms have increasingly adopted technology to enhance business operations and create investment efficiencies, ideally broadening market access and increasing returns.

- This use of technology does not come without risks, however.

- The SEC views the use of AI in a securities context as a potential threat to consumers, particularly when applied in novel contexts.

- As Chair Gensler has stated, "[g]iven the scalability of these technologies and the potential for firms to reach a broad audience at a rapid speed, any resulting conflicts of interest could cause harm to investors in a more pronounced fashion and on a broader scale than previously possible".

SEC Proposed Rules

- The SEC contends that the proposed rules expand upon existing legal norms.
- The proposed rules require firms to assess whether their use of certain technologies in engaging with investors poses a conflict of interest, prioritizing the firm's interests over those of investors.
- These rules would require firms to eliminate or mitigate such conflicts, allowing them to utilize tools tailored to the specific technologies they employ.
- Finally, the proposed rules require firms to maintain written policies and procedures aimed at ensuring adherence to these rules.

Robo-advisers

- In addition to the SEC's recent efforts to regulate the use of AI, the SEC has focused for several years on a growing number of investment advisory firms that have begun offering investment advice through digital platforms using proprietary algorithms instead of traditional human advisors.
- Robo-adviser services are being offered through fully automated means in which the customer only interacts with the digital platform, as well as through hybrid means in which human services are paired in varying degrees with the digital offerings.
- In both circumstances, the advisory firm is able to offer their services to clients at a lower cost by offering them passive investments that do not need a human adviser and the fees that come with it.
- The popularity of robo-advisers is growing rapidly, with major financial firms such as Charles Schwab and Goldman Sachs developing online advisory platforms.
- Robo-advisers "create personalized investment portfolios, obviating the need for stockbrokers and financial advisers".

Robo-advisers

- Supporters of digital investment advice have argued that robo-advisers are able to handle all of an investor's portfolio needs while keeping costs low and avoiding potentially costly human error and bias that can occur in investment services.

- Properly constructed and tested robo-advisers may also help to reduce the incidence of fraud and errors in the provision of advisory services by eliminating humans that are at times driven by greed or other nefarious motives.

- Critics argue that while robo-advisers may be able to complement the services provided by traditional human advice, the former will never replace the latter due to the personal element provided by traditional investment services and the nuances involved in investment advice.

- Regardless of one's opinion on the virtues of robo-advice, the growth of the industry raises a unique set of regulatory questions such as how exactly robo-adviser services fit under existing supervisory frameworks.

- While the SEC has not adopted new rules that are tailored to robo-advisers, SEC guidance has sought to guide robo-advisers compliance with existing laws.

- The SEC has encouraged robo-advisers to provide clear disclosures, in addition to what is usually required of advisers on the Form ADV, including information about the adviser's specific business model and related risks.

Robo-advisers

- The SEC has noted the disclosures should include "[a] statement that an algorithm is used to manage individual client accounts" and "[a] description of the particular risks inherent in the use of an algorithm to manage client accounts".
- The SEC believes the disclosures help to familiarize customers with how robo-advisers make investment determinations and what specific risks are inherent with such a business model.
- The SEC believes that risks include issues related to algorithms, such as problems with automatic rebalancing of client accounts, or the possibility that an algorithm may not have the capacity to address prolonged changes in market conditions.
- While robo-advisers bring added efficiency, the technology presents unique problems which in the SEC's view justify additional disclosures.
- A robo-adviser should carefully consider the disclosures it plans to make to its customers.
- The disclosures should be based on the list provided in the SEC's guidance and any unique factors in its product offerings that may create risks beyond what is already noted.

Trust But Verify

- Like traditional investment advisers, robo-advisers must comply with Rule 206(4)-7 of the Advisers Act. Rule 206(4)-7 requires advisers to establish an internal compliance program to ensure compliance with the Advisers Act.
- Such compliance includes developing policies and procedures "reasonably designed to prevent violations of the Advisers Act" while taking into consideration the nature of the firm's operations and the specific risks.
- The SEC guidance notes the robo-adviser business model is unique, raising novel compliance concerns.
- Such concerns include the increased risks created by the robo-adviser providing advisory services over the internet.
- The risks should be addressed in the adviser's written policies and procedures and in disclosures to the client regarding changes in the underlying algorithm and the ongoing prevention and detection of cyber security threats.
- The SEC believes robo-adviser services have unique compliance requirements that go beyond the traditional requirements under the Advisers Act.
- Robo-advisers must be cognizant of the risks associated with their products and services and must design a compliance program that addresses those issues with sufficient particularity and present forth a plan for continued protections as the underlying technology continues to develop.

Rogue Programs

- The issues that befell Knight Capital Group in August of 2012 provide a clear example of what can happen when algorithms are not properly tested and monitored.
- Due to an undetected error in the software behind their market-making platform, the group lost $440 million in 30 minutes.
- The error caused erratic trades to be made on nearly 150 different stocks, buying high and selling low.
- The error caused a loss that was larger than Knight's market cap of $296 million at the time, putting the firm's future in jeopardy.
- Firms can reduce to the likelihood of such issues through effective testing and monitoring procedures.
- Robo-advisers should use caution as they develop the algorithms and software that underlie their services.
- The SEC has focused on the importance of testing and monitoring algorithms as a key component of an effective compliance program.
- Robo-advisers must focus on the algorithms that are the basis of their service offerings and should subject the algorithms to critical testing and monitoring to ensure clients are not improperly advised or that their funds are not misused.

CFTC Wants Answers

- On January 25, 2024, the CFTC published an RFC, in which it articulated its approach to the regulation of the use of AI by CFTC-regulated entities.
- The CFTC wanted to determine: (i) how AI was being used by commodity market participants; (ii) the inherent risks of use of this technology by such participants; (iii) what the CFTC should do in response to the proliferation of AI; and (iv) how the use of AI fits within the existing regulatory framework established by the CFTC, the National Futures Association and prevailing market practices.
- In the RFC, the CFTC recognized entities and registrants, (collectively "CFTC regulated entities") and other market participants are increasingly exploring and using AI and related technologies.
- The CFTC noted the "use of AI may lead to significant benefits in derivatives markets, but such use may also pose risks relating to market safety, customer protection, governance, data privacy, mitigation of bias, and cybersecurity, among other issues".
- The RFC is part of an effort by the CFTC to monitor the adoption of AI by CFTC-regulated markets.
- The RFC was also prompted, in part, by AI-related guidance issued by the White House which issued an Executive Order ("Executive Order") encouraging federal agencies, such as the CFTC, 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".

AI Risks in CFTC-regulated Markets

- The CFTC noted the predictions, recommendations, or decisions made by AI may create or heighten risks that vary based on the specific application of AI.
- If not responsibly managed, these risks could cause significant harms.
- The CFTC noted the use of AI in trading applications could contribute to inappropriate trading behavior or market disruptions; AI-based customer interactions could lead to unintended biases and deceptive or misleading communications; and when used for any critical business process, AI could exacerbate risks to operational resiliency.
- The CFTC acknowledged that while AI may present unique challenges to CFTC-regulated entities' ability to identify and manage certain risks, not all of the potential risks associated with the use of AI in CFTC-regulated markets are unique to AI.
- The CFTC noted the types of potential risks can appear similar because AI, like other technologies, processes, tools or models, does not change the underlying activity for which it is being used but the manner in which the activity is being conducted.

AI Risks in CFTC-regulated Markets

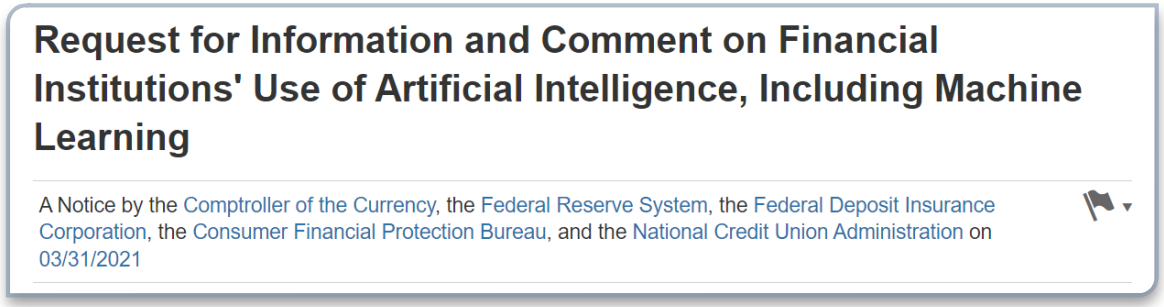
- The CFTC concluded the complexity and autonomy of some AI, deployed in a context of ever-increasing datasets and computing power, also presents unique challenges to CFTC-regulated entities in identifying and managing risks.
- Some of these unique challenges may relate to the ability to explain the results produced by AI.
- Use of an AI model may introduce risks if the predictions, recommendations or decisions made by the AI model cannot be fully explainable.

An Emerging Regulatory Focus at the OCC

- In a joint *Request for Information*, the prudential bank regulators (FDIC, Fed, OCC, NCUA, CFPB) sought industry feedback on the use of AI in banking. They identified several key use cases:

  1. *Flagging unusual transactions*
  2. *Personalization of customer services*
  3. *Credit decisions*
  4. *Risk management*
  5. *Textual analysis*
  6. *Cybersecurity*

- The regulators also flagged a number of significant regulatory concerns — *more on that later….*



The WOPR and the OCC

- Like the WOPR ("War Operation Plan Response") program in the movie War Games, which was based on a quaint massive computer system used by the U.S. military, many banks are reliant on systems that are cyber brethren to the WOPR.
- Unfortunately, the OCC is charged with the supervision of banks that use these metaphorical cyber dinosaurs.
- As banks explore the use of AI, the OCC faces a combination of technologies that are analogous to Agent Smith (AI) and the T-Rex from Jurassic Park (legacy bank systems).
- The OCC, along with its sister prudential regulators the FDIC and the Fed, have long embraced the concept of "responsible innovation" – a policy balancing act recognizing the need to continually evolve as an industry to meet customer demand for financial services without sacrificing the safety and soundness of the U.S. financial system.
- In the fall 2023 publication of the OCC's semiannual risk report, the OCC identified AI as a "special topic in emerging risk".
- The OCC appropriately identified technological advancements in AI and the opportunities available to banks to leverage this technology to improve risk management controls, enhance data analytical techniques, and combat money laundering and other fraudulent activities.
- However, the OCC also recognized that technological innovation also came with heightened challenges and risks related to over-reliance on large data sets, unintended bias, consumer data privacy and third-party vendor risk.

OCC Regulation of the Use of AI

- The potential benefits of AI are significant so long as banks appropriately navigate this balancing act; as with any significant technological innovation deployed at a bank, regulators will certainly scrutinize the implementation to ensure that the bank continues to operate in a safe manner.

- Consistent with existing supervisory guidance, banks are expected to use a risk-based approach when deploying AI such that the bank's use of AI is commensurate with the complexity and risk profile of the bank's business activity that supports AI usage.

- Specifically, a bank considering AI should have policies, procedures and controls in place that enable it to identify, measure, monitor and control risks arising from AI use as they would for the use of any other technology or business activity.

- In other words, technological advances do not preclude the bank from complying with existing regulation and supervisory expectation and, despite the level of automation that technology may impart to a bank, a bank is never permitted to simply rely on AI to meet its supervisory and compliance burdens.

- Although existing guidance may not expressly address AI use, the supervision risk management principles contained in OCC issuances provide a framework for banks that implement AI to operate in a safe, sound and fair manner.

Compliance Uses for AI in Banking

- **Identification and verification of customers**: In the context of remote onboarding and authentication, AI, including biometrics, machine learning, and liveness detection techniques, can be used to perform micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis.

- **Monitoring of the business relationship and behavioral and transactional analysis**:

  - Unsupervised machine learning algorithms: Group customers into cohesive groupings based on their behavior, which will then create controls that can be set more adequately based on a risk-based approach (ex: transaction threshold settings), allowing a tailored and efficient monitoring of the business relationship.
  - Supervised machine learning algorithms: Allow for a quicker and real time analysis of data according to the relevant AML/CFT requirements in place.

- **Alert scoring**: Helps focus on a pattern of activity and issue notifications or need for enhanced due diligence.

- **Identification and implementation of regulatory updates**: Machine Learning techniques with natural language processing (NLP), cognitive computing capability, and robotic process automation (RPA) can scan and interpret big volumes of unstructured regulatory data sources on an ongoing basis to automatically identify, analyze and then shortlist applicable requirements for the institution; or implement (to a certain extent) the new or revised regulatory requirements (via codification and generation of implementation workflows) so regulated entities can comply with the relevant regulatory products.

- **Automated data reporting (ADR)**: Use standardized reporting templates using automated digital applications (data pooling tools) making the regulated entities underlying granular data available in bulk to supervisors.

Supervisory Expectations

- Mr. Greenfield identified several key supervisory expectations that the OCC has for banks that use AI:

Risk-based supervision

- The OCC expects a bank to have well-designed compliance management systems and risk management controls to address AI use in banks.
- Banks are expected to follow a risk-based approach and tailor their systems to the individual risk profile of the bank as well as the bank's scope of activities using AI.
- For example, banks – large or small – intending to deploy AI enterprise-wide would be expected to comply with heightened prudential standards and have more robust risk and compliance controls to ensure that AI use is performed in a safe manner given the risk profile of the bank.
- Systems should be in place to enable banks to conduct appropriate due diligence and risk assessments when evaluating new activities that utilize AI.

Supervisory Expectations

Model risk management

- In 2021, the OCC issued a statement related to model risk management in the context of BSA/AML compliance, as well as broader revisions to the OCC Comptroller's handbook regarding sound model risk management practices.

- It is likely that AI algorithms and processes would fall within this model risk management guidance and, as a result, a bank should ensure that its controls (e.g., due diligence, risk management/assessment, governance and monitoring) are appropriate and comply with OCC guidance.

Third-party risk management

- The OCC expects banks to have an effective third-party risk management program that includes robust due diligence, effective contract management and ongoing oversight of third parties.

- For AI, this typically means that a bank should have controls over the deployment of the technology in the bank and should monitor the third party's performance, including its use of data, on an ongoing basis.

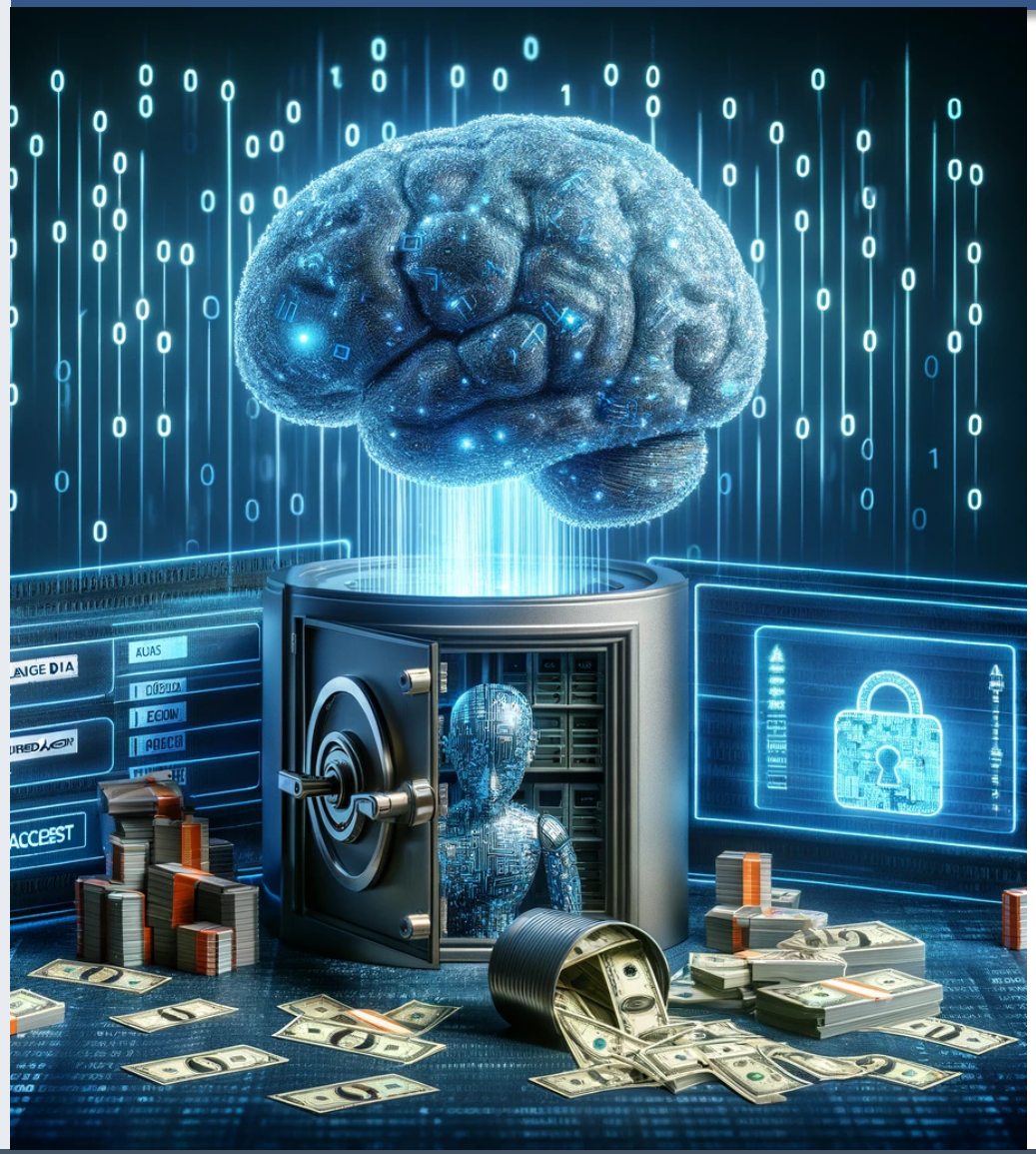
Supervisory Expectations

Responsible use of data

- The OCC expects banks to understand the data inputs flowing through AI systems and evaluate the resultant output against any potential unfair or discriminatory bias that could result in adverse consumer actions or even failure to comply with certain statutes such as the obligations set forth under the Community Reinvestment Act.

- As a result, banks should be cautious with over-reliance on large data and alternative sets powering the AI engine and build controls around maintaining data integrity to ensure actions taken as a result of AI-predicted outcomes are not only performed in a safe and sound manner but also in a manner that does not run afoul of consumer protection laws.

Third-party Providers



- When using third-party AI solutions, banks are expected to maintain oversight and accountability, ensuring third-party providers meet the same standards of safety and soundness.
- The use of third-party AI increases exposure to cyber risks. Banks need to enhance cybersecurity measures and protect sensitive customer data processed by AI systems.
- *How would your bank respond if your GLBA data was being provided in response to AI Chatbot queries*?

Presenter Biographies

RICHARD B. LEVIN

Richard is chair of the FinTech and Regulation Practice and was one of the first lawyers to focus on the regulation of blockchain and digital assets. He is considered a thought leader in the FinTech space. Richard brings his experience as a senior legal and compliance officer on Wall Street and in London to bear in advising clients on corporate, FinTech, securities, and regulatory issues. A problem-solver by nature, he has been advising FinTech clients on legal and regulatory issues since the start of electronic trading in the late 1990s. His practice focuses on helping financial services and technology clients identify and address regulatory issues as they build their businesses.

Richard's practice focuses on the representation of early stage and publicly traded companies in the FinTech space, including investment banks, broker-dealers, investment advisers, peer-to-peer lending platforms, digital currency trading platforms, alternative trading systems (ATSs), exchanges, and custodians. He represents these firms before the U.. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), the U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC), state regulators, and Congress. Richard has represented clients before regulators in Australia, Canada, France, Germany, Hong Kong, Ireland, Japan, Singapore, South Korea, and the United Kingdom. His current and past clients include leading national financial institutions, multinational financial services holding companies, leading firms in the FinTech space, and institutions engaging in global investment banking, investment management, securities, and other financial services with institutional clients.

Richard has been identified by Chambers and Partners as one of the leading lawyers in the Blockchain and Cryptocurrencies category since the inception of the category. He has been recognized by Chambers for his knowledge on regulatory matters, great relationships with regulators, for helping clients push the boundaries of the FinTech sector, and for his advice on matters such as broker-dealer licensing and alternative trading systems. Richard is routinely quoted by leading publications including Bloomberg, the New York Times, Reuters, and the Wall Street Journal and is a frequent speaker at conferences around the world on the regulation of FinTech, blockchain, and digital assets.

Presenter Biographies

KEVIN TRAN

Kevin assists financial institutions and technology clients with financial regulatory, securities, and corporate matters. He focuses on the representation of early stage, mid-stage, and publicly traded FinTech companies focused on blockchain technology, digital assets, and cryptocurrencies, including broker-dealers, digital asset and currency trading platforms, digital asset custodians, alternative trading systems, and securities exchanges and swap execution facilities.

BOBBY WENNER

Bobby counsels financial services and technology firms on financial services regulatory and corporate matters. He focuses on the representation of financial technology companies working with blockchain, tokenization, digital assets, and cryptocurrencies, including broker-dealers, alternative trading systems (ATS), digital asset and currency trading platforms, digital asset issuers and custodians, securities exchanges, and derivatives trading platforms including swap execution facilities.

Contact Details

To learn more about our FinTech and Regulation practice, or to contact a member of our team, click here or visit our website at nelsonmullins.com.

To learn more about this presentation, please contact:

Richard B. Levin
Chair FinTech and Regulation Practice
1400 Wewatta Street
Suite 500
Denver, CO 80202
Tel. 303.583.9929
richard.levin@nelsonmullins.com

Kevin Tran
Partner
1222 Demonbreun Street
Suite 1700
Nashville, TN 37203
Tel. 615.664.5322
kevin.tran@nelsonmullins.com

Bobby Wenner
Of Counsel
1400 Wewatta Street
Suite 500
Denver, CO 80202
Tel. 303.583.9907
bobby.wenner@nelsonmullins.com

About This Publication

- Nelson Mullins provides this material for informational purposes only.
- The material provided herein is general and is not intended to be legal advice.
- Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues.
- Receipt of this material does not establish an attorney-client relationship.
- Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.