CFTC

COMMODITY FUTURES TRADING COMMISSION

AI Day: Technology Advisory Committee Meeting – May 2, 2024

TAC Sponsor
Commissioner Christy Goldsmith Romero

CFTC

COMMODITY FUTURES TRADING COMMISSION

Opening Remarks

Commissioner
Christy Goldsmith Romero

Commissioner
Kristin N. Johnson

Commissioner
Summer K. Mersinger

Commissioner
Caroline D. Pham

CFTC

COMMODITY FUTURES TRADING COMMISSION

AI Day Presentations

Takeaways from Market Automation and Issues to Watch

Kirsten Wegner

May 2, 2024

CFTC Technology Advisory Committee

RISE OF AI & KEY ISSUES PRESENTED

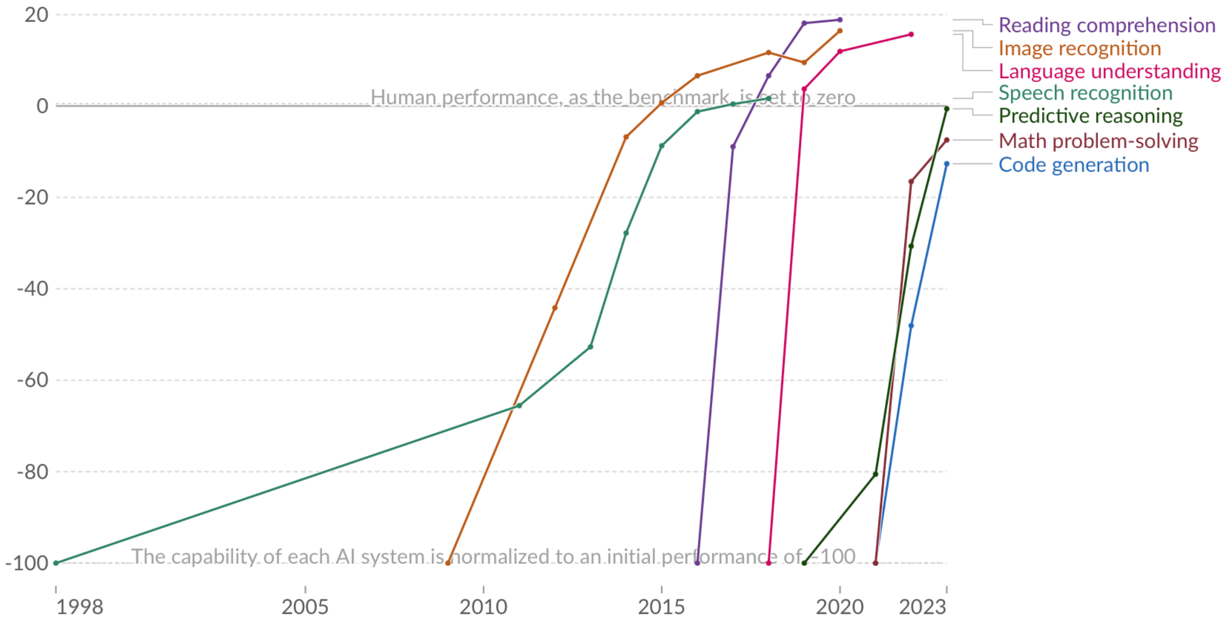
- Exponential growth of computer power since 1950s; AI industry value projected to reach ~ $300 billion by 2026.

- Need for Responsible Innovation in AI:
  - AI as *tool* for humans;
  - Data as *raw material* for AI;
  - Level-set on AI nomenclature – so all on same 2;
  - Governance of AI models, protocols to fair, transparent, safe and secure;
  - Accountability – where does the buck stop – identifying gaps in existing regulation; internal audits;
  - Third party service providers – data and AI systems- accountability.

Test scores of AI systems on various capabilities relative to human performance

Our World in Data

Within each domain, the initial performance of the AI is set to –100. Human performance is used as a baseline, set to zero. When the AI's performance crosses the zero line, it scored more points than humans.



Data source: Kiela et al. (2023) OurWorldInData.org/artificial-intelligence | CC BY

Note: For each capability, the first year always shows a baseline of –100, even if better performance was recorded later that year.

- Although chart shows in some areas, AI is approaching human intelligence, many areas where AI still struggling and/or unable to surpass human thought processes.

AUTOMATION – EXAMPLES OF USE CASES

Financial Services Industry:

- CFO Tools - Dynamic pricing/goods; modeling out workflows, demand;
- Speech Recognition – analysis/ earnings calls – to listen to multiple earnings calls at once, draft summaries, analysis.
- Pattern recognition; loss mitigation, detection of unusual patterns, e.g. detecting spoofers or manipulators; cyber-crime detection;
- Analyzing alternative data – e.g. satellite images of store parking lots; shipping traffic; social media sentiment, etc.

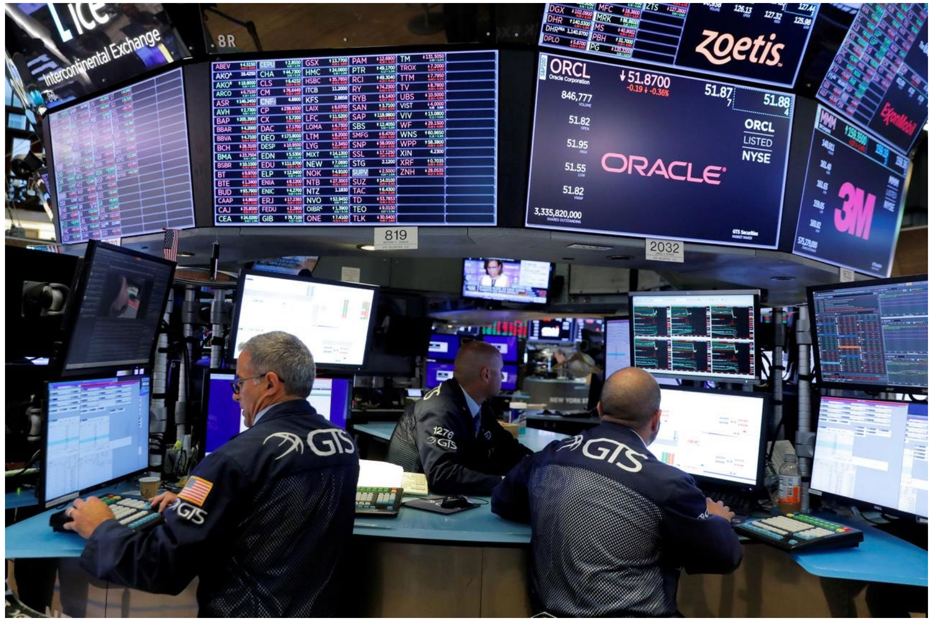
Brokers (e.g. Futures Commission Merchants):

- Administrative/back end – automating paper-based processes (processing orders, depositing checks, searching and retrieving documents); document review (e.g. contracts, prospectuses);
- Smart Order Routing –machine learning for for smart order routing, price optimization, best execution, and optimal allocations of block trades.
- Cash and liquidity management – e.g. intra-day liquidity needs, peak liquidity demands, working capital requirements,
- KYC - customer identification/ financial crime monitoring;
- Risk management -surveillance and monitoring of data (text, video, image, voice, etc.) for patterns and anomalies.

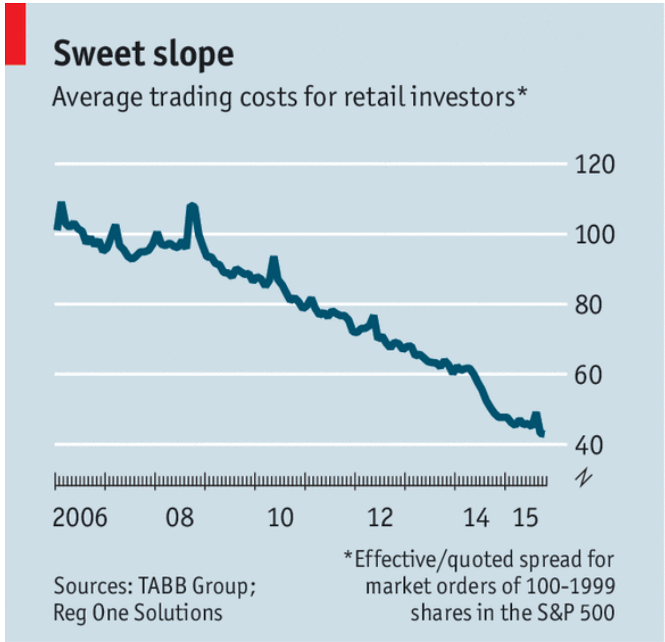
USE CASE: MARKET AUTOMATION – ALGO TRADING

Then: 1980s - Floor brokers and traders /"specialists" relied on written notes and verbal communication.

Now: Automated traders execute trades using electronic orders and computer algorithms as tools to humans to match bids and asks.



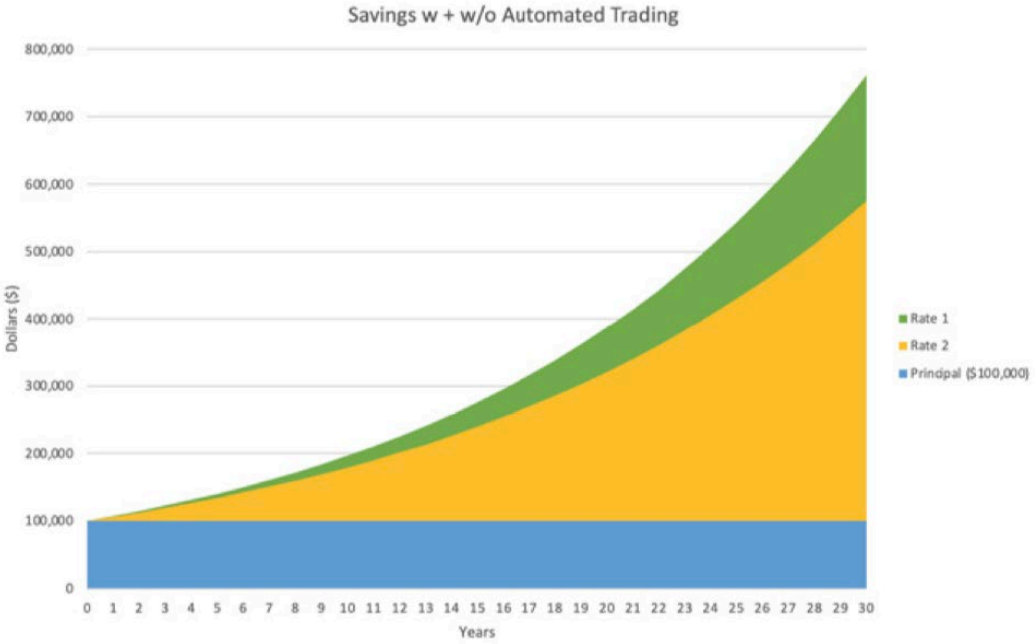
BENEFIT: SAVINGS/ EFFICIENCIES FOR INVESTORS



Economist.com

- The average trading cost for investors has **fallen by more than 50 percent over a decade** as a result of market automation.

- Investments in a retirement account will deliver a **30 percent higher return** over a 30-year period than in pre-market automation. As a result of automated trading technology, middle class investors can retire two years earlier. See: MMI Study (2022)



CHALLENGES: LESSONS LEARNED DURING MARKET AUTOMATION

(1) Leveraging Tech to Detect Bad Actors - As bad actors become more sophisticated, automated trading firms and regulators must leverage technology to detect for those committing illegal activity (spoofing, market manipulation, front-running); need for private firms to surveillance against and detect/turn in to FINRA or other regulators;

(2) Glitches / "Flash Crashes" – technology not immune from a glitch – and need for solutions e.g. development of circuit breakers– for market stability;

(3) "Data" – liquid gold – the raw material for automated trading systems – and questions arising regarding cost, access, monetization – see the "war of wall street" between SROs and brokers in decade of litigation;

(4) Nomenclature - difficulty in finding definitions – e.g. "HFT" … in AI context, hard to define AI – e.g. some people using simple regression analysis and claim to be using AI…how to know that someone who claims to be using AI, actually is, and vice versa.

(5) Importance of Information-Sharing Between Industry and Regulators – to educate on issues (e.g. source code, how viewed as a trade secret)

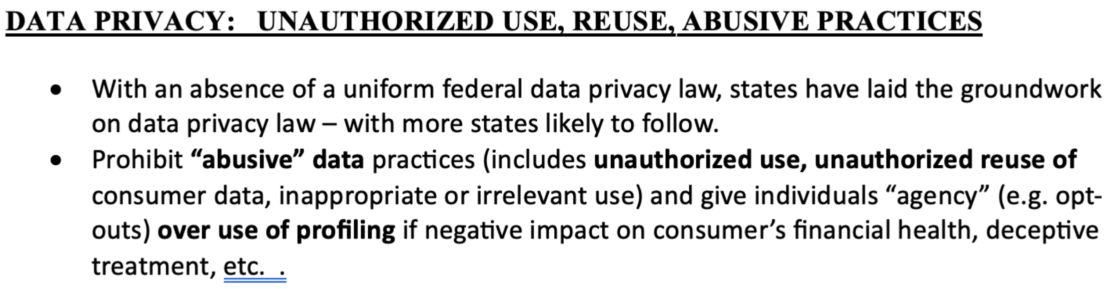
FEDERAL BIPARTISAN PROPOSAL RE-EMERGES ON DATA, RAW MATERIAL OF AI SYSTEMS

- Data privacy is important building block for responsible AI - no federal data privacy law.
- Among recent bipartisan federal data/ AI proposals:

  (1) **American Privacy Rights Act** (APRA), Sen. **Maria Cantwell** (D-WA) and Rep. **Cathy Rodgers** (R-WI) – federal privacy framework – preempts some state privacy laws, but does not preempt other state laws related to consumer protections, civil rights, data breach notification, student/employee privacy, other (April 2024);

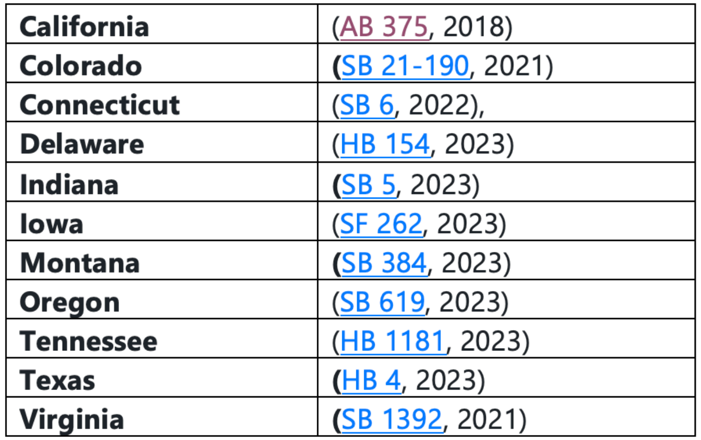
  (2) **Financial Artificial Intelligence Risk Reduction**, Act **Sen. Warner** (D-VA) and Sen. **John Kennedy** (R-LA) - require financial regulators to address uses of AI-generated content that could disrupt financial markets.
- Data – Policy questions include (but not limited to)
  - **Transparency** - how data is being used in an AI system
  - **Consumer rights** – consent (to use, re-use data); to view, correct, or delete data; can't use data to discriminate
  - **Data anonymity v confidentiality** (with identifier for regulators), data minimization
  - **Data broker registry** – third party vendors
  - **Data integrity** – e.g. how we know what data is real v AI generated (e.g. watermarks for provenance); how to validate (including unstructured) data sets going in to algorithms?

STATES: LABORATORIES OF DEMOCRACY



DATA PRIVACY: UNAUTHORIZED USE, REUSE, ABUSIVE PRACTICES

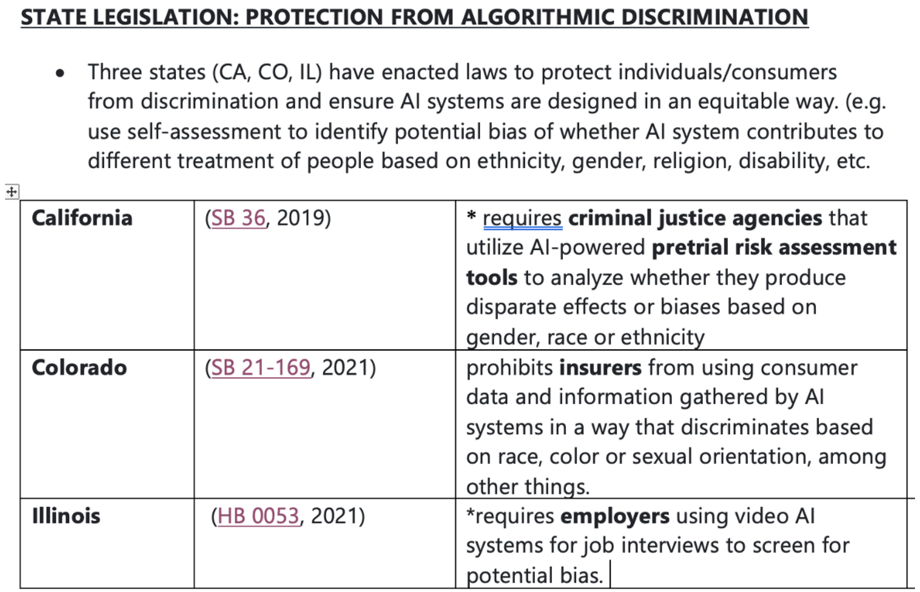
- With an absence of a uniform federal data privacy law, states have laid the groundwork on data privacy law – with more states likely to follow.
- Prohibit **"abusive" data** practices (includes **unauthorized use, unauthorized reuse of** consumer data, inappropriate or irrelevant use) and give individuals "agency" (e.g. opt-outs) **over use of profiling** if negative impact on consumer's financial health, deceptive treatment, etc. .



California	(AB 375, 2018)
Colorado	**(**SB 21-190, 2021)
Connecticut	(SB 6, 2022),
Delaware	(HB 154, 2023)
Indiana	**(**SB 5, 2023)
Iowa	(SF 262, 2023)
Montana	**(**SB 384, 2023)
Oregon	(SB 619, 2023)
Tennessee	(HB 1181, 2023)
Texas	**(**HB 4, 2023)
Virginia	**(**SB 1392, 2021)

April 2024: **new state laws:**

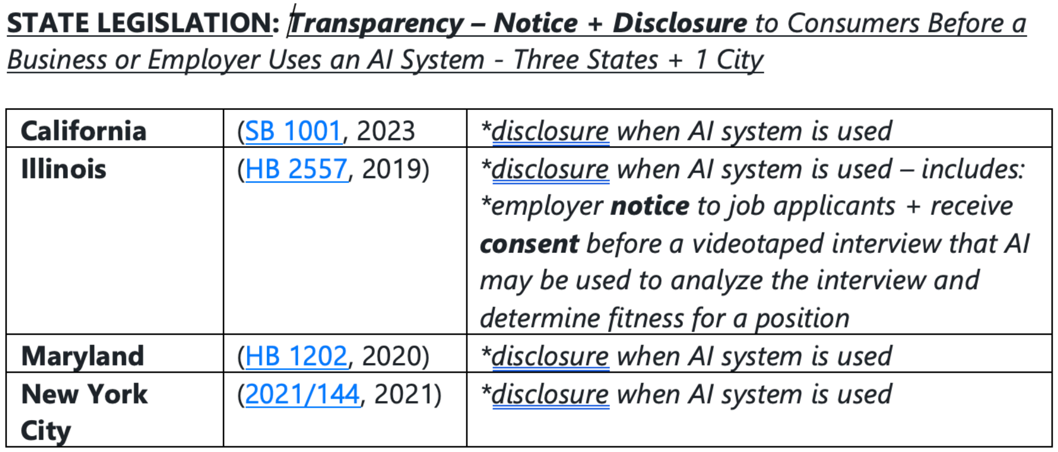
- Kentucky (April 3, 2024) **- Consumer Data Rights Act** (follows VA model)
- Maryland (April 6, 2024) **Maryland Online Data Privacy Act of 2024**



STATE LEGISLATION: PROTECTION FROM ALGORITHMIC DISCRIMINATION

- Three states (CA, CO, IL) have enacted laws to protect individuals/consumers from discrimination and ensure AI systems are designed in an equitable way. (e.g. use self-assessment to identify potential bias of whether AI system contributes to different treatment of people based on ethnicity, gender, religion, disability, etc.

California	(SB 36, 2019)	* requires **criminal justice agencies** that utilize AI-powered **pretrial risk assessment tools** to analyze whether they produce disparate effects or biases based on gender, race or ethnicity
Colorado	(SB 21-169, 2021)	prohibits **insurers** from using consumer data and information gathered by AI systems in a way that discriminates based on race, color or sexual orientation, among other things.
Illinois	(HB 0053, 2021)	*requires **employers** using video AI systems for job interviews to screen for potential bias.



STATE LEGISLATION: ***Transparency – Notice + Disclosure*** *to Consumers Before a Business or Employer Uses an AI System - Three States + 1 City*

California	(SB 1001, 2023	**disclosure* *when AI system is used*
Illinois	(HB 2557, 2019)	**disclosure when AI system is used – includes:* **employer* ***notice*** *to job applicants + receive* ***consent*** *before a videotaped interview that AI may be used to analyze the interview and determine fitness for a position*
Maryland	(HB 1202, 2020)	**disclosure when AI system is used*
New York City	(2021/144, 2021)	**disclosure when AI system is used*

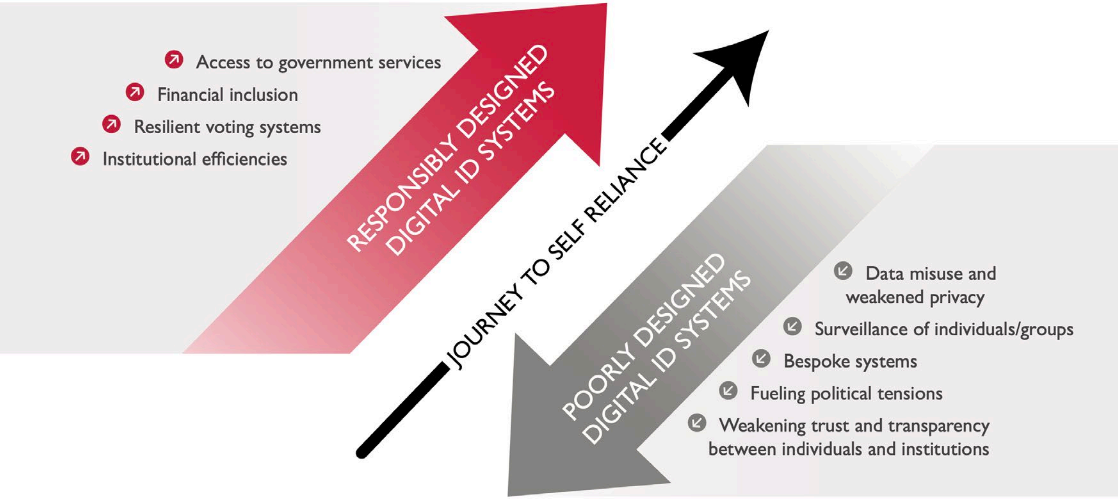
Modern Markets Initiative

STATES: DIGITAL IDS – POTENTIAL USE CASES

- States, rather than federal government, issue drivers licenses/digital IDs.

- Some have called for the establishment of a “federal ID” or “federal drivers license” - see USAID graphic of responsibly designed digital ID system.

- In the question of privacy verses anonymity, some have argued that a digital ID is one way to provide a unique identifier for a consumer while maintaining anonymity.


Access to government services
Financial inclusion
Resilient voting systems
Institutional efficiencies
RESPONSIBLY DESIGNED DIGITAL ID SYSTEMS
JOURNEY TO SELF RELIANCE
POORLY DESIGNED DIGITAL ID SYSTEMS
Data misuse and weakened privacy
Surveillance of individuals/groups
Bespoke systems
Fueling political tensions
Weakening trust and transparency between individuals and institutions

- Use cases: accountability, data protection, monetization, evaluating fairness/bias; transparency, data dividends (i.e. idea in California, Minnesota).

ACCOUNTABILITY & AI

- Bad actors – examples:
  - Market manipulators, spoofers, front-runners; cyber-attackers; national security threats,
  - Fraud, impersonators; Misinformation, deepfakes.
- Private sector – building trust and accountability:
  - Build best practices for AI governance models, protocols to be fair, transparent, safe and secure. Innovate (e.g. watermarks, blockchain for provenance). Build trust with public.
  - Information-sharing within industry and with regulators on best practices, technology, work on nomenclature/vocabulary to have shared frame of reference; if breach or cyber-attack, lessons learned; identify any areas where there are gaps in existing regulation.
- Regulators:
  - Build workforce/ tech capacity to tackle AI, promote more forums of information-sharing;
  - Promote accountability, transparency, and flexible principles-based approach for AI;
  - Third party service providers (for data, and AI systems) may play growing role, engage for information-sharing and ensuring accountability.

THANK YOU

Questions?
Please contact me at:

Kirsten.Wegner@gmail.com

OCCIP

Office Of Cybersecurity
& Critical Infrastructure
Protection

EXECUTIVE ORDER 14110: SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE

4.3 (ii) Within 150 days of the date of the order, the Secretary of the Treasury shall issue a public report on best practices for financial institutions to manage AI- specific cybersecurity risks.

U.S. Regulatory Framework for AI in Financial Services

- Financial sector supervisors have existing risk management and control principles that are applicable to AI:
  - Risk management and governance
  - Model risk management
  - Technology risk management
  - Data management
  - Compliance and consumer/investor protection
  - Third-party risk management
  - Securities market access risk management
  - Insurance

AI Use Cases: Cybersecurity and Fraud Protection

- Cybersecurity
  - Endpoint protection, intrusion detection/prevention, data loss prevention (DLP), network appliances, etc.
- Risk Management and Fraud Prevention
  - AI/ML for anomaly detection and mapping fraudulent behavior patterns
  - Augmentation of labor intensive/process-oriented tasks

AI in the Financial Services Sector: Cybersecurity and Fraud Protection

- Overall, the sector is taking a cautious approach to Generative AI adoption and is leveraging existing practices (e.g., NIST's AI Risk Management Framework) to support enterprise policies
- Mixed use of in-house and third-party AI systems that varies by institutional size
  - Larger institutions are leveraging commercial and proprietary data for model training, while smaller institutions heavily rely on vendor data
- Financial institutions desire better information sharing across the sector to improve data aggregation and AI/ML fraud detection models

Cybersecurity and Fraud Threats

- Threat actor use of AI
  - Sophisticated social engineering, malicious code generation, reduction in vulnerability discovery time, and disinformation
- Identity impersonation and synthetic IDs
- Underlying threats to AI systems (e.g., data poisoning, model extraction, and data leakage)
- Third-party risk
  - Data security and privacy challenges

Best Practices for Managing AI-Specific Cyber Risk

- Situate AI within existing enterprise risk management programs
- Develop and implement an AI framework
- Integrate risk management functions for AI
- Evolve the Chief Data Officer (CDO) role & map the data supply chain
- Ask the right questions of vendors
- Survey NIST's Cybersecurity Framework (CSF) to identify opportunities for AI use
- Implement risk-based tiered MFA
- Pick the right tool for the job & risk tolerance
- Cybersecurity best practices apply to AI systems

Next Steps: Challenges and Opportunities

1. **Need for a common AI lexicon.** There is a lack of consistency across the sector in defining "artificial intelligence."
2. **Addressing the growing capability gap.** There is a widening gap between large and small financial institutions when it comes to developing in-house AI systems.
3. **Narrowing the fraud data divide.** As financial institutions work with their internal data to develop fraud models, large institutions hold a significant advantage because they have far more historical data.
4. **Regulation remains an open question.** As different financial-sector regulators at the state, federal, and international levels consider regulations for AI, there is concern about regulatory fragmentation.
5. **Expansion of NIST AI Risk Management Framework.** The NIST AI RMF could be expanded and tailored to include more content on AI governance and risk management related to the financial services sector.

Next Steps: Challenges and Opportunities

6. **Best practices for data supply chain mapping and “nutrition labels”.** The financial sector would benefit from the development of best practices for data supply chain mapping and a standardized description for vendor-provided AI systems and data providers.
7. **Decipher explainability for black box AI solutions.** The sector would benefit from additional research and development on explainability solutions for black-box systems like generative AI.
8. **Gaps in human in capital.** A set of best practices for less-skilled practitioners on how to use AI systems safely and role-specific AI training would help manage the growing workforce talent gap.
9. **Untangling digital identity solutions.** Robust digital identity solutions can help financial institutions combat fraud and strengthen cybersecurity.
10. **International coordination.** The path forward for regulation of AI in financial services remains an open question internationally. Treasury will continue to engage with foreign counterparts on the risks and benefits of AI in financial services.

Other Treasury AI Work

- Treasury remains focused on a range of AI-related matters outside the scope of this report, including:
  - Continued monitoring of the deployment of AI in the financial sector to identify risks that could undermine the sector's integrity and stability
  - Developing Treasury's internal AI use cases
  - Exploring opportunities to engage the public on the sufficiency of existing regulatory frameworks and the impacts to consumers and investors by financial institutions' use of AI

OCCIP | Office of Cybersecurity and Critical Infrastructure Protection

QUESTIONS?

OCCIP
Office Of Cybersecurity
& Critical Infrastructure
Protection

October xx, 2022

OCCIP

Office Of Cybersecurity
& Critical Infrastructure
Protection

CFTC

COMMODITY FUTURES TRADING COMMISSION

AI Report Consideration

RESPONSIBLE ARTIFICIAL INTELLIGENCE

IN FINANCIAL MARKETS: OPPORTUNITIES, RISKS & RECOMMENDATIONS

*A Report of the Subcommittee on Emerging and Evolving Technologies,
Technology Advisory Committee (TAC) of the
U.S. Commodity Futures Trading Commission*

CFTC Subcommittee on Evolving and Emerging Markets

Members

Name	Title	Affiliation
Dr. Nicol Turner Lee (Co-Chair)	Senior Fellow and Director, Center for Technology Innovation	The Brookings Institution
Todd Smith (Co-Chair)	Director, Information Systems	National Futures Association
Dan Awrey	Professor of Law	Cornell Law School
Cantrell Dumas	Director, Derivatives Policy	Better Markets
Dan Guido	CEO and Founder	Trail of Bits
Carole House	Executive in Residence, and Senior Fellow, the Atlantic Council	Terranet Ventures Inc.
Ben Milne	Founder and CEO	Brale
Dr. Francesca Rossi	AI Ethics Global Leader	IBM
Joe Saluzzi	Partner, Co-Founder, and Co-Head of Equity Trading	Themis Trading
Dr. Steve Suppan	Senior Policy Analyst	Institute for Agriculture and Trade Policy
Corey Then	Vice President and Deputy General Counsel, Global Policy	Circle
Dr. Michael Wellman	Professor, Electrical Engineering and Computer Science	University of Michigan
Todd Conklin	Chief AI Officer, and Deputy Assistant Secretary of Cyber	U.S. Treasury Department

***The Subcommittee also acknowledges the research support of Jack Malamud and Joshua Turner from the Brookings Institution as well as Michael Schorsch from NFA. ***

Report Objectives

- **Provides a comprehensive overview of AI adoption and use by entities under the jurisdiction of the CFTC.**
  - ***For whom?*** Exchanges, clearinghouses, and others acting as futures commission merchants and swap dealers, as well as managed funds and advisors, introducing brokers, retail forex exchange dealers, and data repositories – *collectively known* as "CFTC-registered entities."

- **Offers definitions of 'Responsible AI,' governance, and technical terms as they apply to the CFTC-registered entities, and global financial markets overall.**

- **Assesses the executive, legislative, and regulatory U.S. policy frameworks, and the current global guidance.**

Report Objectives

- **Proposes a series of ‘use case scenarios’ (real and hypothetical) for the application of AI from fraud detection to super-manipulative chatbots.**

- **Explores risk management strategies of AI tools and describes possible paths forward for CFTC and registered entities.**

- **Concludes with proposed recommendations for CFTC staff, registered entities, and other partner federal agencies.**

Key Definitions

Artificial Intelligence

- machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments

AI Safety

- an area of machine learning research that aims to identify causes of unintended behavior in machine learning systems and develop tools to ensure these systems work safely and reliably

Foundational Model

- any AI model that is trained on broad data that can be adapted to a wide range of downstream tasks

Generative AI

- the class of AI models that emulate the structure and characteristics of training data to generate derived synthetic content. This can include images, videos, audio, text, and other digital content

?

Five typical proper

Fairness, Robustne
Transparency, Expl
and Privacy

AI Risks and Management of them Among CFTC-Registered Entities

There are certain widely identified and well-known AI Risks in industry, government and academia.

Types of AI Risks

Lack of Transparency	• Not knowing or being able to explain an AI model decision making process
Poor Data Quality	• Data “overfitting” or “poisoning” of AI models
Mishandling of Data	• Sensitive data handling mishaps or misuse
Fairness	• Reproduce or compound biases
Model Concentration	• Widely deployed and utilized AI foundational models

Partial List of Use Cases

TRADING AND INVESTMENT

- Investment research
- Algorithmic and High-Frequency Trading

CUSTOMER COMMUNICATIONS, ADVICE AND SERVICE

- Marketing
- Customer Acquisition and Retention

RISK MANAGEMENT

- Margin model monitoring
- Collateral and liquidity optimization

REGULATORY COMPLIANCE

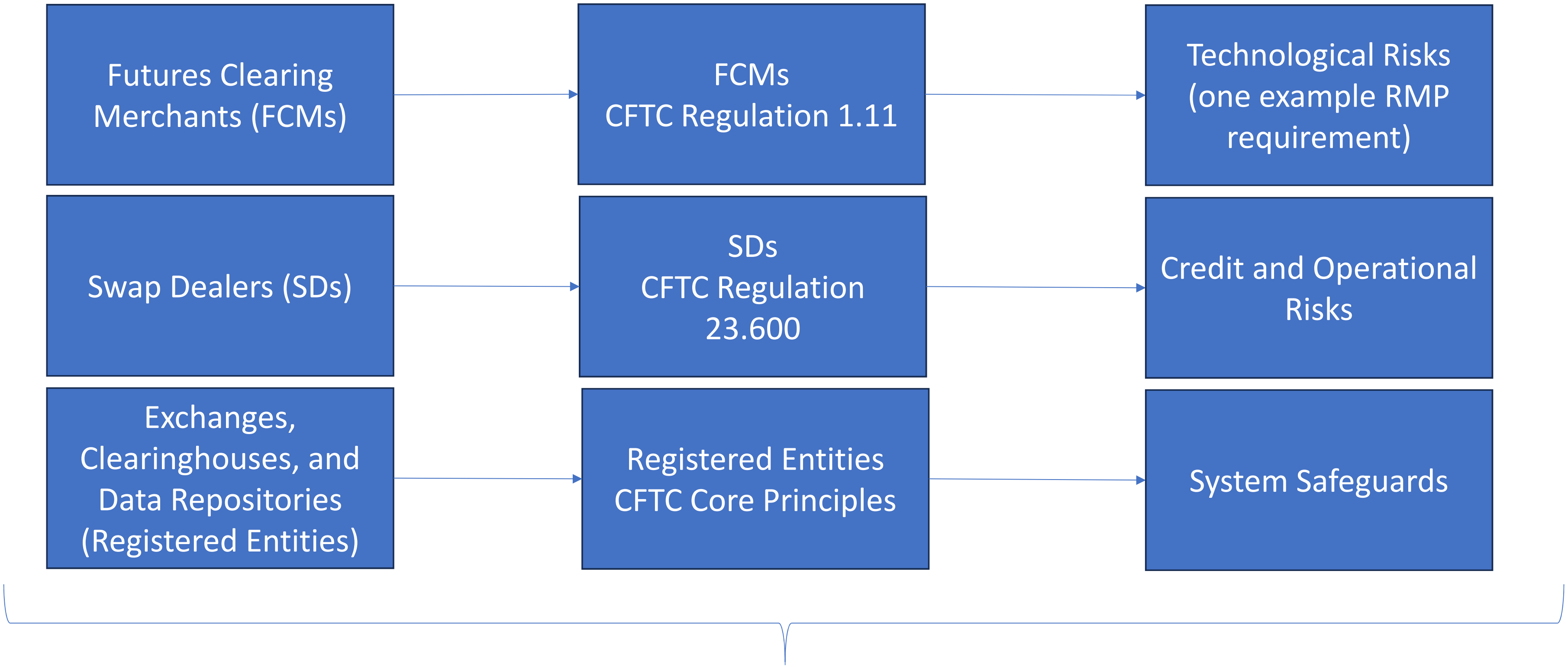
- Market Surveillance
- KYC/AML
- Capital and margin calculations

BACK OFFICE / OPERATIONS

- Trade verification, reconciliation, and reporting

AI Risk Management Framework

Existing Requirements Risk Management Programs



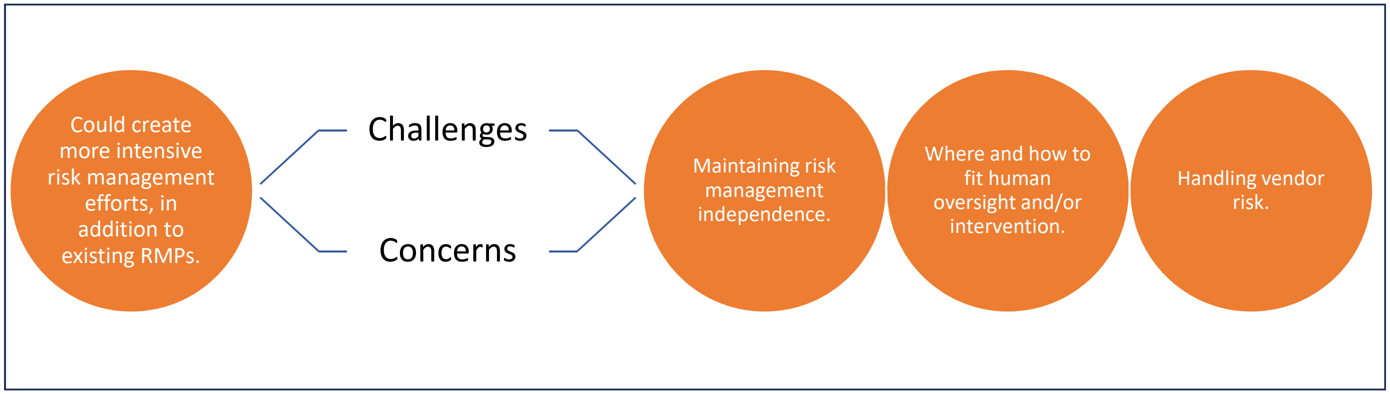
Futures Clearing Merchants (FCMs)	FCMs CFTC Regulation 1.11	Technological Risks (one example RMP requirement)
Swap Dealers (SDs)	SDs CFTC Regulation 23.600	Credit and Operational Risks
Exchanges, Clearinghouses, and Data Repositories (Registered Entities)	Registered Entities CFTC Core Principles	System Safeguards

CFTC Engagement to Identify Potential Gaps

AI Risk Management – Path Forward

Whether and to what extent firms should incorporate an AI-specific risk-management function into their existing risk management structures.

Adding to existing Risk Management Programs has challenges and concerns.



Could create more intensive risk management efforts, in addition to existing RMPs.

Challenges

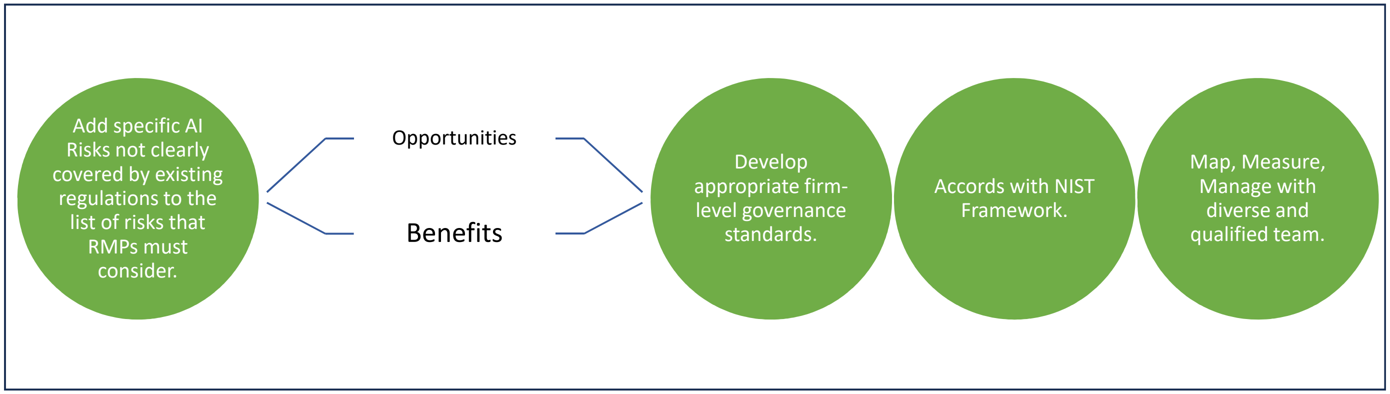
Concerns

Maintaining risk management independence.

Where and how to fit human oversight and/or intervention.

Handling vendor risk.

Opportunities and benefits of a governance-based approach to initial AI risk management efforts.



Add specific AI Risks not clearly covered by existing regulations to the list of risks that RMPs must consider.

Opportunities

Benefits

Develop appropriate firm-level governance standards.

Accords with NIST Framework.

Map, Measure, Manage with diverse and qualified team.

Related Risk Management Issues

- **Training data**
  - ➢ Quality of data
  - ➢ Type of data
  - ➢ Representativeness of data

- **The placement of humans**
  - ➢ Human-in-the-loop (HITL)
  - ➢ Human-on-the-loop (HOTL)

- **The growth of the talent pipeline**
  - ➢ Recent OMB Guidance for agency Chief AI Officers
  - ➢ Staff capacity building around AI expertise
  - ➢ Budget implications

- **The spreading of misinformation**
  - ➢ Super-manipulative models

Types of AI Governance and Applications

First Type

- The lifecycle of the model, which includes data collection, data labelling, model training, system deployment.

Second Type

- Corporate policies and regulations on the use of AI in regulated and unregulated industries.

Third Type

- Strategies for identifying and mitigating technical and socio-technical risks.

Fourth Type

- Governmental intervention, or national and global regulation.

Fifth Type

- Strict guidance and guidelines on the types of technologies, i.e., generative AI.

AI Governance

High Level Considerations

- **Have policies and procedures to do with mapping, measuring and managing AI Risks.**
- **Ensure individuals responsible for oversight of AI systems have appropriate qualifications and training.**
- **Qualify informed decision-making by having a diverse team (NIST notes diversity in terms of demographics, as well as expertise, experience and academic disciplines).**

AI Governance

High Level Considerations

- Have robust engagement with relevant internal and external AI actors.
- Establish clear communication and feedback processes for personnel with actionable knowledge of the development, foundational training, and adaptive training of AI systems.
- Address risks arising from involvement of outside service providers, especially third-parties.

Our Recommendations

One

The CFTC should host a public roundtable discussion and CFTC staff should directly engage in outreach with CFTC-registered entities to seek guidance and gain additional insights into the business functions and types of AI technologies most prevalent within the sector.

Our Recommendations

Two

The CFTC should consider the definition and adoption of an AI Risk Management Framework (RMF) for the sector, in accordance with the guidelines and governance aspects of the NIST, to assess the efficiency of AI models and potential customer harms as they apply to CFTC-registered entities, including but not limited to governance issues.

Our Recommendations

Three

The CFTC should create an inventory of existing regulations related to AI in the sector and use it to develop a gap analysis of the potential risks associated with AI systems.

- ➢ **The purpose of the gap analysis would be to determine compliance relative to further opportunities for dialogue on their relevancy, and potential clarifying staff guidance or potential rulemaking.**

Our Recommendations

Four

The CFTC should strive to gather and establish a process to gain alignment of their AI policies and practices with other federal agencies, including the SEC, Treasury, and other agencies interested in the financial stability of markets.

Our Recommendations

Five

The CFTC should work toward engaging staff as both ‘observers’ and potential participants in ongoing domestic and international dialogues around AI, and where possible, establish budget supplements to build the internal capacity of agency professionals around necessary technical expertise to support the agency’s endeavors in emerging and evolving technologies.

Thank you for your consideration of the final Report and Recommendations

Questions and Answers

CFTC

COMMODITY FUTURES TRADING COMMISSION

Closing Remarks