CFTC

COMMODITY FUTURES TRADING COMMISSION

December 10, 2024 Market Risk Advisory Committee Meeting

Commissioner
Caroline D. Pham

Commissioner
Christy Goldsmith Romero

Chairman
Rostin Behnam

Commissioner
Kristin N. Johnson

Commissioner
Summer K. Mersinger

CFTC

COMMODITY FUTURES TRADING COMMISSION

Welcome and Opening Remarks

CFTC

COMMODITY FUTURES TRADING COMMISSION

Opening Keynote Remarks

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section One: Market Structure Subcommittee

Perspectives on Treasury Markets

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section One: Market Structure Subcommittee

Recommendations on the Treasury Cash-Futures Basis Trade and Effective Risk Management Practices

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section Two: Central Counterparty (CCP) Risk & Governance Subcommittee
Part 1: Ensuring Cyber Resilience and Preparedness for Third-Party Service Providers

Perspectives on Cyber Resilience

FIA Cyber Risk Taskforce

- In March 2023, FIA formed a Cyber Risk Taskforce in response to a ransomware attack on a single third-party service provider.
- In September 2023, the Taskforce released an after-action report with recommendations for improving the industry's ability to withstand the disruptive impacts of a cyberattack or outage.
- In December 2023, FIA formed the Industry Resilience Committee (IRC) as recommended by the Taskforce. The IRC acts as a trusted forum for key stakeholders to discuss cyber incident management, resilience planning and recommend best practices for the industry.

FIA Industry Resilience Committee:

The IRC is made up of a cross-section of SMEs across market participant types, including experts in information security, technology and operations. The initial priorities set forth by the IRC and FIA have been on the following:

- **Incident Response:** Serving as a trusted group for sharing information and coordinating response during an ongoing cyber incident or other type of outage.
- **Sector Engagement:** Engage with sector-wide groups on cyber and operational resilience coordination efforts
- **Operational Resilience:** Focus on the Three R's: **Response** - coping with the immediate impact of a breach; **Recovery** - rebuilding and restoring systems; and **Reconnection** - reconnecting to market infrastructures.

Improving Operational Resilience:

The IRC is working to produce a questionnaire for Exchanges/CCPs with the aim of assisting their members in recovering clearing, settlement, reference and risk data during an incident, broken out into the four sections below:

- Incident Response Plans and Notification to Clearing Members / ISVs.
- Access to Clearing Records & Data
- Data Format
- Data Retention & Availability of Historical Data

Their responses are intended to be shared directly with their clearing members and Third-Party Service Providers.

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section Two: Central Counterparty (CCP) Risk & Governance Subcommittee
Part 1: Ensuring Cyber Resilience and Preparedness for Third-Party Service Providers

Recommendations on Derivatives Clearing Organization System Safeguards Standards for Third-Party Service Providers

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section Two: Central Counterparty (CCP) Risk & Governance Subcommittee
Part 2: Legal Entity Identifiers at the Beneficial Account Holder Level

Recommendations on Legal Entity Identifiers at the Beneficial Account Holder Level

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section Three: Future of Finance Subcommittee Presentation

December 10, 2024

Managing Artificial Intelligence-Specific Cybersecurity Risk in the Financial Services Sector

Todd Conklin

Deputy Assistant Secretary for Cybersecurity and Critical Infrastructure Protection

Chief Artificial Intelligence Officer

U.S. Department of the Treasury

Traditional AI in the Financial Services Sector

- The financial services sector has been using traditional AI for many years
- 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

How Financial Services Sector Firms are Adopting new AI Technologies

- 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
- The use of AI to fight fraud is a potential growth area for many institutions. 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

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.

Workstream Summaries

Primary Workstreams

AI Lexicon and Terminology

- Lexicon containing definitions of key AI terms.

AI Enhanced Fraud

- Catalog risks and threats to fraud and scam ecosystem, as enabled by AI and mitigation points.
- Create data sharing roadmap, document hurdles to sharing.
- Recommendations for reinforcement learning to counter scams and fraud.

CRI Financial Sector AI Profile

- Financial sector-specific AI control framework based on the NIST AI Risk Management Framework (RMF) and aligned to the CRI Profile.

May Merge into Primary Workstreams

Financial Services AI Nutrition Labeling

- Plain-language guide to enable practitioners to examine datasets for any number of deficiencies.
- Best practices for practitioners to determine completeness and clarity of data used to generate AI products.

Identity and Authentication

- Develop best practices for financial institutions and technology companies to mitigate identity-related risks tied to AI-generated impersonations.
- Improve the ability of financial institutions to trust and to digitally validate government ID documents and other digital attributes during enrollment and authentication processes.
- Identify steps government can take to close the gap between physical and digital government credentials. Enable identity information to be validated against government "reservoirs of truth."

Workstream Summaries

Primary Workstreams

AI Lexicon and Terminology

- Develop a lexicon containing definitions of key AI terms.
- Treasury is leading the workstream; workstream members include regulators, sector members, and AI practitioners.

AI Enhanced Fraud

- Catalog risks and threats to fraud and scam ecosystem, as enabled by AI and mitigation points.
- Create data sharing roadmap, document hurdles to sharing.
- Recommendations for reinforcement learning to counter scams and fraud.

CRI Financial Sector AI Profile

- Financial sector-specific AI control framework based on the NIST AI Risk Management Framework (RMF) and aligned to the CRI Profile.

May Merge into Primary Workstreams

Identity and Authentication

- Develop best practices for financial institutions and technology companies to mitigate identity-related risks tied to AI-generated impersonations.
- Improve the ability of financial institutions to trust and to digitally validate government ID documents and other digital attributes during enrollment and authentication processes.
- Identify steps government can take to close the gap between physical and digital government credentials. Enable identity information to be validated against government "reservoirs of truth."
- Workstream is partnering with the Better Identity Coalition.

Workstream Summaries

Primary Workstreams

Explainability

- The workstream will aim to meet the expectations of explainability by delivering trusted, reliable, and interpretable outcomes through the alignment of core enterprise risk management concepts focused on applications to cyber, fraud, and operational resilience issues.
- The goal will be to capture the coordinated elements necessary to provide evidence for the explainability approach and satisfy the concept in the appropriate context and purpose.
- The Bank Policy Institute is leading the workstream.

Accountability

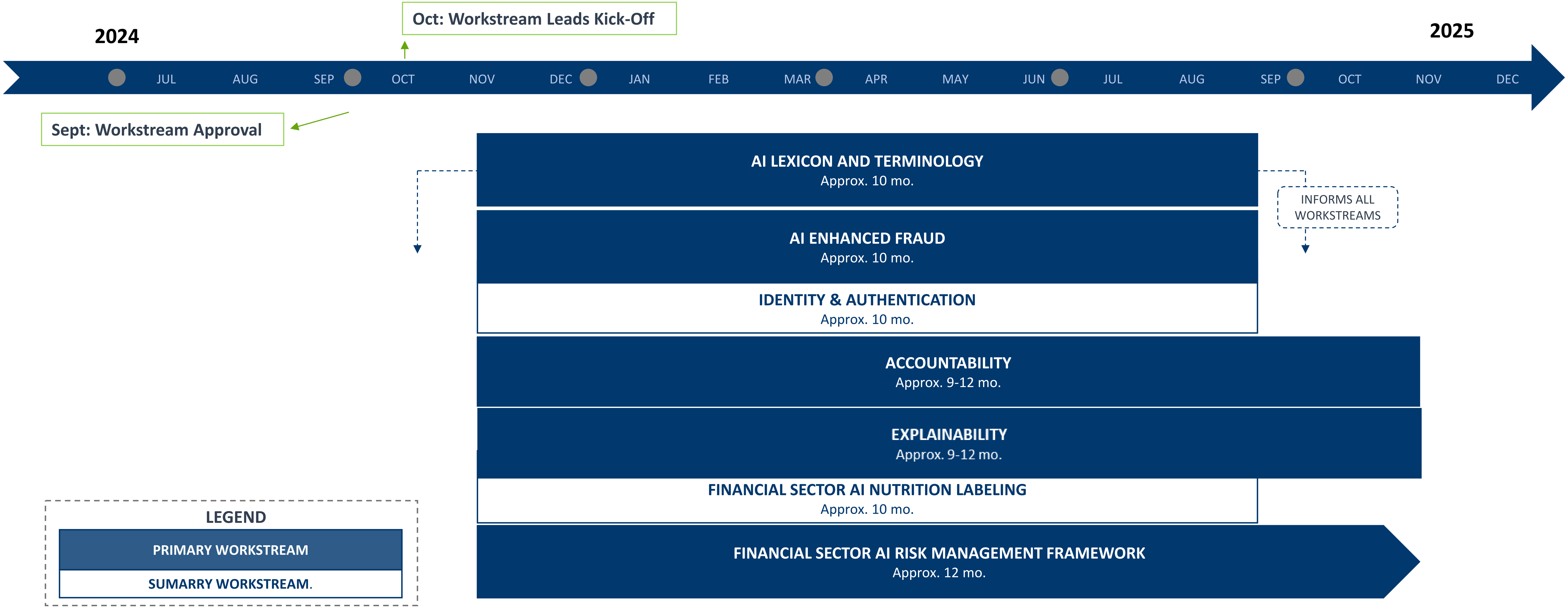
- The workstream will explore what financial institutions need to do to successfully use AI models in a responsible manner.
- The workstream's goal will be to discuss what a financial institution is responsible for while using AI algorithms.

May Merge into Primary Workstreams

Financial Services AI Nutrition Labeling

- Plain-language guide to enable practitioners to examine datasets for any number of deficiencies.
- The workstream's goal is to document best practices for practitioners to determine completeness and clarity of data used to generate AI products.
- PNC Bank is leading the workstream.

Tentative Timeline



Oct: Workstream Leads Kick-Off

Sept: Workstream Approval

AI LEXICON AND TERMINOLOGY
Approx. 10 mo.

INFORMS ALL WORKSTREAMS

AI ENHANCED FRAUD
Approx. 10 mo.

IDENTITY & AUTHENTICATION
Approx. 10 mo.

ACCOUNTABILITY
Approx. 9-12 mo.

EXPLAINABILITY
Approx. 9-12 mo.

FINANCIAL SECTOR AI NUTRITION LABELING
Approx. 10 mo.

FINANCIAL SECTOR AI RISK MANAGEMENT FRAMEWORK
Approx. 12 mo.

LEGEND

PRIMARY WORKSTREAM

SUMARRY WORKSTREAM.

Thank you

CFTC

COMMODITY FUTURES TRADING COMMISSION

Section Four: Climate-Related Market Risk Subcommittee Presentation

CFTC

COMMODITY FUTURES TRADING COMMISSION

Closing Remarks

CFTC

COMMODITY FUTURES TRADING COMMISSION

Adjournment