Public Statements & Remarks

Opening Remarks of Commissioner Kristin Johnson: Regulators Roundtable on Financial Markets Innovation and Supervision of Emergent Technology

July 14, 2025

It is truly my pleasure to welcome you all today to the Regulators Roundtable on Financial Markets Innovation and Supervision of Emergent Technology. My sincere and tremendous gratitude to everyone who has gathered here in London today. This year marks the third year that I have had the privilege of convening an exceptional group of senior prudential and market regulators representing diverse jurisdictions around the world.

Our discussion this afternoon will focus on forces that are rapidly transforming the financial services sector of the global economy with particular emphasis on two elements of the increasingly digitized financial services sector—the integration of artificial intelligence and the threat of cyber risks.

For each of us—whether we're shaping monetary policy, evaluating compliance with current regulatory guidelines, enforcing transparency and accountability in banking, capital markets, derivatives markets or digital asset markets, or supervising the next generation of digital finance platforms—the topics on today's agenda are top of mind.

Today we are continuing the conversations launched during the previous roundtables. Each of these topics have only become more important in the year since we last gathered.

Let's begin with artificial intelligence (AI).[1]

AI in Financial Markets and Financial Markets Regulation

AI holds significant promise for making financial services more inclusive, efficient, and accessible. But its deployment must be underpinned by robust governance, ethical design, and global regulatory collaboration. For global regulatory leadership—including this august group convened today—the challenge is to balance innovation with stability, openness with security, and automation with human oversight.

Improving Accuracy, Efficiency, and Operational Resilience

Evidence suggests that AI improves accuracy, efficiency, and operational resilience and that AI-driven systems may outperform traditional approaches. Some potential applications include:

Fraud Detection and Risk Management

- **Anomaly Detection**: AI systems can detect unusual transaction patterns in real-time, flagging potential fraud or cyber threats more effectively than traditional rule-based systems.

- **Behavioral Biometrics**: Advanced models track behavioral traits (typing speed, swipe patterns) to authenticate users and reduce identity theft.

Process Automation

- **Intelligent Document Processing (IDP)**: AI extracts, classifies, and processes information from unstructured documents (e.g., loan applications, KYC documents), reducing processing time and human error.
- **Trade Surveillance & Market Monitoring**: AI can sift through vast quantities of data to detect signs of market manipulation, insider trading, or compliance breaches with greater precision.

Enhancing Compliance with Regulation and Reducing the Costs of Compliance

AI promises to reduce transaction and compliance costs by dynamically routing orders to the best venues, reducing slippage and lowering transaction costs. Evidence suggests that AI improves accuracy, efficiency, and operational resilience. AI-driven systems may outperform traditional approaches for detecting fraud, managing risks, executing back-office services, verifying identity, surveilling markets for evidence of market manipulation, insider trading, and compliance breaches.

AI also promises to enhance supervisory technology for regulators—automating data collection, analysis, and reporting, reducing frictions with regulatory compliance, and enabling more dynamic regulation at reduced costs. AI may facilitate efficient, faster-paced updating and modernization of regulation. AI may also offer continuous monitoring and enhanced real-time confirmation of compliance, reducing reliance on less frequent, periodic audits, and facilitating market participants and regulators' ability to identify regulatory breaches earlier and potentially reducing the number and size of regulatory breaches.

Reducing Transaction and Compliance Costs

Transaction Costs

- **Smart Routing and Algorithmic Trading**: AI optimizes trade execution by dynamically routing orders to the best venues, reducing slippage and transaction costs.

Compliance and Regulatory Reporting

- **RegTech Solutions**: AI-powered regulatory technology automates data collection, analysis, and reporting, easing the burden of compliance with dynamic regulations.
- **Continuous Monitoring**: AI systems can provide real-time compliance checks rather than periodic audits, leading to faster resolution and fewer regulatory breaches.

Industry Use Cases

While the financial services industry has integrated predictive technologies in risk assessment and predictive analytics for decades, over the last several years, we have witnessed a transformational shift in the diversity of use cases. In 2017, JPMorgan Chase launched a contract intelligence platform that automates review of commercial credit agreements, reducing by hundreds of thousands of hours the human resources annually required to complete credit agreement reviews.[2] HSBC, and a number of other financial institutions, have integrated AI in their transaction monitoring and anti-money laundering (AML) platforms to detect anomalies across millions of transactions in real-time, increasing accuracy in their assessment of suspicious activity reports.[3] Similar to other financial services firms, Mastercard has launched cyber risk and fraud detection software that relies on AI to analyze 75 billion transactions per year to block fraud in milliseconds.[4]

Risks and Considerations for Policymakers

In testimony before Congress, published academic literature, and a series of speeches during my tenure as a Commissioner at the CFTC, I have outlined and encouraged regulators to explore a number of risks and considerations.

For example, we face real concerns around bias in AI models, especially when it comes to lending and underwriting. There is a need for greater transparency and explainability, so that AI driven decisions are subject to the rigorous accountability standards that we typically apply in our supervisory oversight. And as AI becomes more embedded in core infrastructure, cyber resilience becomes a systemic concern, not just an operational one.

There is also the matter of concentration risk. As more institutions rely on a handful of foundational AI models or platforms, we must ask: what happens when those systems fail or are compromised? I outline a few additional risks below:

Bias and Fairness

- **Model Transparency**: AI decisions, especially in lending or insurance, must be explainable to ensure non-discriminatory practices.
- **Data Integrity**: Models are only as good as the data they are trained on—bad data can perpetuate historical inequalities.

Cybersecurity and Resilience

- **Adversarial AI**: As AI becomes embedded in core infrastructure, it's also a target for manipulation—highlighting the need for robust, secure design.
- **Systemic Concentration**: Overreliance on a few AI platforms or vendors could increase systemic vulnerabilities.

Governance and Accountability

- **Model Risk Management**: Institutions must manage the full lifecycle of AI models—development, validation, deployment, and monitoring—with strong oversight.
- **Cross-Border Coordination**: Global consistency in AI governance frameworks will be crucial to avoid regulatory arbitrage and ensure responsible innovation.

Next Steps in Governing AI

Governance—at the firm level and the system level—matters more than ever. Fintechs must invest in model risk management, ethical design, and responsible data practices. Supervisory approaches must evolve to keep pace with the changes occurring in the markets subject to our supervision.

Regulatory agencies in the US are increasingly deploying AI to review large volumes of data and detect emerging risks by identifying outliers. Using AI in this capacity, often referred to as "suptech," may offer regulators more effective tools to combat fraud, market manipulation, illicit finance, money-laundering and other long-standing threats to the integrity of our markets.

Cyber Risks

I have encouraged diverse stakeholders to be mindful of potential cyber risks that may impact individual firms or the broader financial markets ecosystem.[5]

We continue to discuss these risks. As we consider them, let's think about the potential implications of interdependence and the possibility of contagion—the threat that a domino effect of risks may occur at an accelerated speed.

Operational Resilience

Over the past few years, we have made progress in preparing ourselves to take on these challenges. The Commission issued a proposed rule, unanimously supported, to create an operational resilience framework for futures commission merchants, swap dealers, and major swap participants to "identify, monitor, manage, and assess risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations" in December 2023.[6]

Cyber resilience is a critical gateway issue for protecting market integrity, and an area where we need to be "all hands on deck" on both sides of the pond. Cyber resilience is only as strong as its weakest link. As most cyber threats may be launched against financial institutions in many nations, it is important to stay vigilant and collaborate closely on best practices and lessons learned.

Third-Party Risk Management

As I discussed in recent remarks, the Market Risk Advisory Committee that I sponsor at the CFTC has been actively focused on cyber resilience and third-party risk management issues.[7] When the Commission released its proposed operational resilience framework, a subcommittee workstream of the MRAC recognized that there may have been some important gaps in operational resilience with respect to other market participants, such as central counterparties regulated by the CFTC, and took up the mantle to continue to examine areas not fully addressed by the Commission. The CCP Risk & Governance Committee organized recommendations that were presented to the commission that "would improve upon the existing framework and require that derivatives clearing organizations establish, implement, and maintain a third-party relationship management program."[8]

Many aspects of the recommendations were informed by internationally recognized best practices and international standard setting bodies, such as the Bank for International Settlements Principles for Financial Market Infrastructure. Once again, this highlights the importance of international collaboration, in setting the standard for best practices, and for developing policies that are familiar to global market participants.

I look forward to discussing today the latest developments in third party risk management, such as new principles on third-party risk supervision issued by the European Securities and Markets Authority (ESMA) just last month.[9]

International Coordination and Cooperation

As we move across the landscape of emerging technologies and the attendant risks, it is increasingly clear that international cooperation is not optional—it is essential. Innovative technologies and the risks that may arise as a result of digitization are not bound by jurisdictional, territorial, or national boundaries. The threats or risks born in one nation may quickly ripple across continents.

A vulnerability in a third-party service provider can contemporaneously compromise multiple financial institutions. A sophisticated actor can launch a cyber-attack from anywhere in the world, orchestrating the consequences such that they impact any one nation or group of nations simultaneously.

Let me highlight a few ways we are already working together on these issues, and where we must go further.

First, harmonizing regulatory expectations.

We need to align our supervisory approaches across jurisdictions to ensure that cyber risk is being addressed consistently. The Financial Stability Board, CPMI-IOSCO, and other international standard setting bodies have already announced important principles—but implementation must be global, not fragmented.

Standards like NIST, ISO 27001, and the FSB's cyber incident response guidance should form the backbone of our shared expectations. It is worth exploring mutual recognition of cyber audits and certifications for third-party providers, especially cloud platforms.

Second, information sharing.

Timely, secure, and actionable intelligence must flow across borders—not just between regulators, but also with the private sector. There are institutions that are helping to build these bridges, but we need to enhance real-time alert systems and threat-sharing protocols. Silence, in the cyber domain, is a vulnerability.

Third, we must strengthen crisis response and recovery.

Too often, we focus on prevention. But in today's threat landscape, we must assume that breaches will occur—and focus on how we respond.

That means building interoperable incident response plans. Conducting joint cyber drills and tabletop exercises simulations and establishing trusted communications channels that can activate instantly in the event of a cross-border incident.

Fourth, we must tackle concentration risk and supply chain vulnerabilities.

Many of our institutions rely on the same cloud providers, fintech APIs, and software stacks. We need a coordinated approach to supervising these critical third parties—through shared resilience testing, pooled audits, and transparent incident reporting.

And finally, we must invest in cyber capacity building, especially in emerging and developing economies. Because in a globally interconnected system, our resilience is only as strong as the weakest link. Let us support these markets with the tools, training, and frameworks they need—not just to defend themselves, but to contribute to the global cyber defense ecosystem.

In Conclusion — Looking Ahead

The cyber threat landscape is evolving quickly—AI-powered attacks, deepfakes, quantum computing threats, and vulnerabilities in decentralized finance are no longer theoretical.

To meet these challenges, we must act together—with speed, with coordination, and with trust. This is no small ask, and we can't do it alone.

Let us make cybersecurity a shared responsibility. Let us foster the partnerships—public and private, domestic and international—that are essential to securing our financial future.

Because in today's world, cyber resilience is not just a technology issue—it is a financial stability imperative.

Finally, our convenings and conversations must continue. Trust can be a competitive advantage if we let it—a most potent tool in our toolbox to help us unlock the potential of new technology while also maintaining effective governance structures that give us the confidence and stability to keep moving forward.

I am hopeful as we continue to convene, as regulators, and with the broader communities we serve, that we can develop standards and best practices that can be relied on around the globe.

I look forward to hearing the different thoughts and approaches that will be shared today on these issues that are top of mind for our markets globally.

---

[1] The thoughts and perspectives that I share with you today are my own; they are not the views and perspectives of my fellow Commissioners, the Commission, or the staff of the CFTC.

[2] JP Morgan COIN: A Banks Side Project Spells Disruption for the Legal Industry, Harvard Business School Digital Initiative (Nov 13, 2018), https://d3.harvard.edu/platform-rctom/submission/jp-morgan-coin-a-banks-side-project-spells-disruption-for-the-legal-industry/ (https://www.cftc.gov/Exit/index.htm?https://d3.harvard.edu/platform-rctom/submission/jp-morgan-coin-a-banks-side-project-spells-disruption-for-the-legal-industry/).

[3] Jennifer Calvery, Harnessing the power of AI to fight financial crime, HSBC (June 10, 2024), https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime (https://www.cftc.gov/Exit/index.htm?https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime).

[4] Mastercard accelerates card fraud detection with generative AI technology, Mastercard (May 22, 2024), https://www.mastercard.com/us/en/news-and-trends/press/2024/may/mastercard-accelerates-card-fraud-detection-with-generative-ai-technology.html (https://www.cftc.gov/Exit/index.htm?https://www.mastercard.com/us/en/news-and-trends/press/2024/may/mastercard-accelerates-card-fraud-detection-with-generative-ai-technology.html).

[5] *See, e.g.*, Keynote Remarks of Commissioner Johnson for Governing Data at Iowa Innovation and Business Law Center and Yale Law Journal of Law & Technology at Yale Law School: Twin Peaks—Emerging Technologies (AI) and Critical Third Parties (Apr. 4, 2025), https://www.cftc.gov/PressRoom/SpeechesTestimony/opajohnson16 (https://www.cftc.gov/PressRoom/SpeechesTestimony/opajohnson16); Opening Remarks of Commissioner Kristin N. Johnson at GAIM Ops AI Summit: Using AI To Combat Cybersecurity and Fraud Risks (Apr. 7, 2025), https://www.cftc.gov/PressRoom/SpeechesTestimony/opajohnson17 (https://www.cftc.gov/PressRoom/SpeechesTestimony/opajohnson17).

[6] CFTC, Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4706 (proposed Jan. 24, 2024).

[7] Commissioner Kristin N. Johnson's Keynote Remarks at the CCP AGM 2025: Addressing Cyber-Risks, Managing Critical Third-Party Relationships, and Reinforcing CCP Resilience (June 19, 2025), https://www.cftc.gov/PressRoom/SpeechesTestimony/opajohnson21 (https://www.cftc.gov/PressRoom/SpeechesTestimony/opajohnson21).

[8] Id.

[9] Principles on third-party risks supervision, ESMA (June 12, 2025), https://www.esma.europa.eu/sites/default/files/2025-06/ESMA42-1710566791-6103_Principles_on_third-party_risks.pdf. (https://www.esma.europa.eu/sites/default/files/2025-06/ESMA42-1710566791-6103_Principles_on_third-party_risks.pdf)

-CFTC-