U.S. COMMODITY FUTURES TRADING COMMISSION

MARKET RISK ADVISORY COMMITTEE

(MRAC) MEETING

Wednesday, March 8, 2023

9:33 a.m.

Commodity Futures Trading Commission

Three Lafayette Centre

1155 21st Street, N.W.

Washington, D.C. 20581

PARTICIPANTS

CFTC COMMISSIONERS AND STAFF:

CHRISTY GOLDSMITH ROMERO, Commissioner

KRISTIN N. JOHNSON, Commissioner and MRAC Sponsor

CAROLINE D. PHAM, Commissioner

BRUCE FEKRAT, Chief Counsel to Commissioner Johnson, MRAC Designated Federal Officer

MARILEE DAHLMAN, Special Counsel, Division of Market Oversight, Alternate Designated Federal Officer

MRAC MEMBERS:

ALICIA CRIGHTON, Chair, Futures Industry Association, Chair of the Board of Directors

ROBERT ALLEN, FMX Futures Exchange, LP, President and Global Head of Fenics Rates

JAMES ANDRUS, California Public Employee's Retirement System, Interim Managing Investment Director

ANN BATTLE, International Swaps and Derivatives Association, Senior Counsel, Market Transitions and Head of Benchmark Reform

PARTICIPANTS (CONTINUED)

MRAC MEMBERS:

STEPHEN BERGER, Citadel, LLC, Managing Director, Global Head of Government & Regulatory Policy

RICHARD BERNER, Clinical Professor of Management Practice in the Department of Finance and Co-Director of the Stern Volatility and Risk Institute

ALESSANDRO COCCO, Federal Reserve Bank of Chicago, Vice President and Head of Financial Markets Group

BISWARUP CHATTERJEE, Citigroup, Managing Director and Head of Innovation for the Global Markets Division

NEIL CONSTABLE, Fidelity, Head of Quantitative Research and Investments

TIM CUDDIHY, Depository Trust and Clearing Corporation, Managing Director, Financial Risk Management

GINA-GAIL FLETCHER, Professor of Law at Duke University School of Law

PARTICIPANTS (CONTINUED)

MRAC MEMBERS:

GRAHAM HARPER, FIA Principal Traders Group, Head of Public Policy and Market Structure at DRW

LINDSAY HOPKINS, Minneapolis Grain Exchange, LLC, Chief Corporate Counsel, MGEX Clearing

DAVID HORNER, London Stock Exchange Group, Chief Risk Officer, LCH Ltd

DEMETRI KAROUSOS, Nodal Exchange, LLC, President and Chief Operating Officer

EILEEN KIELY, BlackRock, Managing Director

ELISABETH KIRBY, Tradeweb Markets, Managing Director and Head of Market Structure

DEREK KLEINBAUER, Bloomberg SEF, LLC, President

ERNIE KOHNKE, Commodity Markets Council, General Counsel, Vitol

PURVI MANIAR, FalconX Bravo, Inc., Deputy General Counsel

CRAIG MESSINGER, Virtu Financial, Inc., Vice Chairman

ANDREW NASH, Morgan Stanley, Managing Director and Head of Regulatory Affairs

PARTICIPANTS (CONTINUED)

MRAC MEMBERS:

ASHWINI PANSE, Intercontinental Exchange, Inc., Head of Risk Oversight for ICE Clear Netherlands and Chief Risk Officer for the North American Clearinghouses

ANDREW PARK, Americans for Financial Reform, Senior Policy Analyst

JESSICA RENIER, Institute of International Finance, Managing Director, Digital Finance

MARNIE ROSENBERG, JPMorgan Chase & Co., Managing Director, Global Head of Central Counterparty Credit Risk and Strategy

TYSON SLOCUM, Public Citizen, Director, Public Citizen Energy Program

PRESENTERS:

HAYDEN ADAMS, Founder and Chief Executive Officer, Uniswap Labs

DAVID BOWMAN, Senior Associate Director, Program Direction Section, Monetary Affairs at the Board of Governors of the Federal Reserve System

PARTICIPANTS (CONTINUED)

PRESENTERS:

EUN YOUNG CHOI, Director of National Cryptocurrency Enforcement Team, U.S. Department of Justice

CAITLIN CLARKE, Assistant National Cyber Director for Planning and Operations, Office of the National Cyber Director

MATTHEW CRONIN, Director of National Cybersecurity, Office of the National Cyber Director

SONJA GIBBS, Managing Director and Head of Sustainable Finance, Institute of International Finance; Member of the Board, the Integrity Council for the Voluntary Carbon Market (The Integrity Council)

MARK HAYS, Senior Policy Analyst, Americans for Financial Reform/Demand Progress

CHRIS HAYWARD, Chairman of Policy and Resources, City of London Corporation

JULIE HOLZRICHTER, Chief Operating Officer, CME Group

PARTICIPANTS (CONTINUED)

PRESENTERS:

LINDA JENG, Chief Global Regulatory Officer and General Counsel, Crypto Council for Innovation

CANDACE KELLY, Chief Legal Officer, Stellar Development Foundation

BRAD LEVY, Chief Executive Officer, Symphony

WALT LUKKEN, President and Chief Executive Officer, Futures Industry Association

CAROLINE MALCOLM, Global Head of Public Policy, Chainalysis, Inc.

TIM MASSAD, Research Fellow Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government, and Director M-RCBG Digital Assets Policy Project, Harvard University

AMANDA OLEAR, Director, Market Participants Division, CFTC

SUYASH G. PALIWAL, Director, Office of International Affairs, CFTC

KIRSTEN ROBBINS, Senior Special Counsel, Office of International Affairs, CFTC

PARTICIPANTS (CONTINUED)

PRESENTERS:

GREG RUPPERT, Executive Vice President, Member Supervision, FINRA

TOM W. SEXTON III, President and Chief Executive Officer, National Futures Association

BRIAN SMITH, Deputy Assistant Secretary for Federal Finance, U.S. Department of the Treasury

VAL SZCZEPANIK, Director, Strategic Hub for Innovation and Financial Technology, U.S. Securities and Exchange Commission

NATHANIEL WUERFFEL, Senior Vice President, Federal Reserve Bank of New York

AGENDA

AGENDA (CONTINUED)

AGENDA (CONTINUED)

P R O C E E D I N G S

MR. FEKRAT: Good morning. As the Market Risk Advisory Committee Designated Federal Officer, it's my pleasure to call this meeting to order.

Before we begin this morning's discussion, I would like to turn to the commissioners who are at the meeting for opening remarks. The chairman has yielded his time to the membership. We will start with Commissioner Johnson, the sponsor of the Market Risk Advisory Committee; followed by Commissioner Goldsmith Romero, who's in New York, I believe; Commissioners Mersinger and Pham. And we'll have, I believe -- I don't think we have it recorded?

CHAIR CRIGHTON: No.

MR. FEKRAT: Okay. Now, so Commissioners Mersinger and Pham, there are some considerations, issues, and we could speak to that later. But now we'll turn to Commissioner Johnson.

COMMISSIONER JOHNSON: Thank you so much, Bruce.

Good morning, everyone. We're so grateful to have so many of you here today joining us. We are anticipating an exciting day.

This is the first Market Risk Advisory Committee meeting of 2023 and our second MRAC meeting under my sponsorship. As our agenda indicates, today we will engage in the CFTC's first public meeting examining recent cyber disruptions that affected cleared derivatives markets.

On January 31, 2023, in a short statement, ION Cleared Derivatives -- a division of ION Markets, a Dublin-based firm -- acknowledged a cybersecurity event had affected some of its services. ION provides trading, clearing, analytics, Treasury, and risk management services for capital markets and futures and derivatives markets. Many market participants, including some significant futures commission merchants, have entered into services agreements with ION for back-office trade processing and settlement of exchange-traded derivatives.

Because of this central role in trade processing, the cyber attack disrupted not only ION's markets, but also the operations of other market participants, triggering a ripple effect across markets. The cyber incident halted deal matching, required affected parties to rely on manual -- shall we say old school -- trade processing, and caused delays in reconciliation and information sharing and reporting, among other challenges.

Recognizing that many affected firms are within the CFTC's remit and subject to the Commission's oversight, I am asking the MRAC membership and invited speakers to engage in a deep-dive discussion exploring cyber threats that create risk management concerns. Specifically, I am asking them to offer informed, expert guidance on two issues.

First, while we have long implemented and enforced cyber risk regulation for registered market participants, we cannot rest on our laurels. Technology is ever evolving. Perhaps equally important, market structure concerns, including concentration and consolidation, require re-evaluating and confirming that our risk management regulation is sufficiently robust to ensure effective cyber risk prevention, business continuity planning, cyber attack mitigation, and general recovery and resilience. Firms should have a day-one plan for responding to cyber incidents.

Second, our economy is a digital economy. Global financial markets indisputably rely on the Internet and Internet of Things. We are now witnessing the deployment of Web 3.0. The salience of third-party service providers and reliance on nonproprietary software for operational mechanics such as trade processing, margin determinations, and data distribution underscore the importance of revisiting our risk management regulations to ensure that the Commission has adequate visibility into the system safeguards of firms impacted -- or firms that may impact the operational integrity of our markets. We must have fit-for-purpose cyber risk management regulations.

In addition to this and opening the conversation this morning, we have as guest speakers members of the Office of National Cyber Director, fellow market regulators, prudential regulators, self-regulatory organizations, academics, public interest advocates, the public, and others as we begin to identify, examine, and explore both the vulnerabilities in our markets and specific policy interventions for consideration by the Commission, best practices for industry participants, and public-private partnerships or industry-engineered initiatives.

Our agenda is ambitious, admittedly, because in addition to thinking carefully about these issues, we will cover MRAC's historic role in delivering first-of-its-kind, unprecedented reports and recommendations. In fact, the service we're providing here in this room is the subject of a hearing before the Senate Ag Committee this morning, where our chair is testifying.

Before we move into the substance of today's meeting, I want to thank our chairman, Commissioners Goldsmith Romero, Mersinger, and Pham for participating today and for their invaluable contributions to this discussion. As the agenda for each of the five advisory committees takes shape, I think it will be increasingly clear that there are common interests in addressing the challenges that face our markets. This common interest will also reveal common ground that may enable us to find consensus and build bridges that lead us on a pathway from the challenges we're facing to effective solutions.

In accord with the statutes governing the advisory committees, I encourage my fellow commissioners and the members of the other advisory committees to consider and coordinate joint meetings that focus on parallel workstreams, leverage the talent and expertise of the resources across the industry and advisory committees and subcommittees, and deliver valuable recommendations that effectively address these issues.

Today, during our meeting, we will hear from a number of distinguished speakers regarding a wide range of topics all relevant to the MRAC's market risk-related mandate, including the areas of emerging technology-oriented risks affecting derivatives and related financial markets. We'll also focus on the subcommittee's productivity, including reports from Central Counterparty Risk and Governance Subcommittee; the Climate-Related Market Risk Subcommittee; the Market Structure Subcommittee; and the Interest Rate Benchmark Reform Subcommittee.

Throughout the course of the day, we've invited special guests to share with us highlights and reflections based on their observations. Our very first opening panel, in fact, reflects the same.

We welcome and anticipate remarks from Tom Sexton, President and Chief Executive Officer of the National Futures Association; Walt Lukken, President and Chief Executive Officer of the Futures Industry Association; Julie Holzrichter of CME; Amanda Olear, Director of Market Participants Division for the CFTC, and Greg Ruppert, Executive Vice President of FINRA.

Alongside their presentations, we anticipate additional presentations from members of the CCP Risk and Governance Subcommittee and our Office of International Affairs.

Later this morning, we'll hear from Chris Hayward, Chairman of Policy and Resources with the City of London Corporation, as well as former CFTC Chair Tim Massad, and current research fellow at the Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government.

Alongside Tim, we'll hear from Val Szczepanik -- I think Bruce is going to correct me on that pronunciation -- Director of the SEC's Strategic Hub for Innovation and Financial Technology; Eun Young Choi, Director of Department of Justice's Innovation and Financial -- sorry, Director of the Department of Justice's National Cryptocurrency Enforcement Team; Mark Hays, senior policy analyst at Americans for Financial Reform; and Alessandro Cocco, Vice President and Head of Financial Markets Group at the Federal Reserve Bank of Chicago.

A second panel of industry participants, whose names I'll not share here because I think Bruce is giving me the elbow, will present on uses that we've not yet considered with sufficient rigor related to digital assets. In particular, distributed digital ledger technologies.

Finally, we will have three reports from the Climate-Related Market Risk, Market Structure, and Interest Rate Benchmark Reform Subcommittees. I'm excited to hear from all of you who will share with us today. I welcome the tremendous knowledge and information that you'll share.

I have to thank each of you for sharing your time with us and your expertise. I'll pause there, and I think we shift to Commissioner Goldsmith Romero.

MR. FEKRAT: Thank you, Commissioner.

We'll turn to remarks from Commissioner Goldsmith Romero. Thank you.

COMMISSIONER GOLDSMITH ROMERO: Thank you. It's so nice to part of this today. I'm sorry I can't be with you in person as I'm in our New York office, but I really wanted to thank the MRAC members for your service, Commissioner Johnson for her leadership of MRAC, Bruce Fekrat and the other staff for putting this together.

I also want to say welcome and thank you to those who are speaking today and give a special shout-out to former Chairman Massad, who he and I worked very, very closely together at Treasury on the TARP program before he came over to the CFTC. So I think I'm probably just following him over to the CFTC in his career path that way. So it's really nice to be working together again.

Global markets face significant market risks from geopolitical events, economic uncertainties, and continued impacts from the pandemic. So the MRAC's objective and scope to advise on systemic issues that impact the stability of markets could not be more timely or necessary. The Commission can really benefit from your advice about market risk, given that the last 3 years have placed systemic stresses on market stability.

The pandemic, supply chain disruptions, a tightened labor market, a difficult interest rate environment, and Russia's war have brought unprecedented systemic risk market issues. The 1-year milestone of Russia's war provides a sober reminder of the substantial risk in the derivatives and commodities markets that arise from geopolitical events. Russia's invasion of Ukraine sent a shock wave, as Ukraine's wheat was cut off, Russian sanctions diverted key commodities, and commodity prices and volatility soared.

Due to a U.S.-led international response and an unseasonably warm winter, many commodities are down from the highs, and commodities markets have proven resilient, as have derivatives markets.

I'm very interested in MRAC members' views about market risk 1 year into the war. How are your financial institutions or other companies thinking about risk related to Russia's war that could impact our markets? Are there things that the Commission should be considering related to geopolitical uncertainty, and how should the markets adapt to become more resilient to that geopolitical uncertainty?

I also seek your advice on how the Commission should be thinking about risk in terms of the high prices, high volatility, and high volume that our markets experienced this past year. Our job as a regulator is to be proactive, to identify and understand risk, to investigate, to study, to root out vulnerabilities in the markets and fix them so that American families, farmers, ranchers, and other end-users don't have to pay the price.

Additionally, I've heard from end-users about economic uncertainty. On Monday, FDIC Chairman Gruenberg spoke about risk to the banking system saying, "First and foremost is the uncertainty about the macroeconomic outlook. There seems to be important trends at work that push the economy in different directions. Maybe that is why there seems to be even less agreement among economists than usual about when the next recession will occur and how severe it will be."

And then he listed specifically "recession uncertainty, inflation, higher and changing interest rates, and structural changes in the economy that create a lot of uncertainty."

So these are challenging issues that have systemic consequences that can impact the stability of our markets. I'm interested in how the members consider these risks for derivatives markets. What does it mean for future liquidity or other areas should this risk impact banks? How can derivatives markets adequately manage these very serious and challenging risks?

These critical systemic issues facing derivatives markets matter to the U.S. economy and matter to American families. I'm grateful for your service and seek your advice on these important market risk issues.

Thank you.

MR. FEKRAT: Thank you, Commissioner Goldsmith Romero.

Commissioner Mersinger is under the weather, and

Commissioner Pham had some delays getting in from New York. I don't know if IT is working with Commissioner Pham to have her remarks.

COMMISSIONER PHAM: Commissioner Pham is on.

MR. FEKRAT: Okay, wonderful. Thank you so much.

Commissioner, if you would?

COMMISSIONER PHAM: Good morning.

Thank you to Commissioner Johnson; Bruce Fekrat, the Designated Financial Officer; and to the many guest speakers and those members in attendance for today's meeting of the Market Risk Advisory Committee. I value your time and contributions.

I am pleased to see that the MRAC is following on to and continuing the important discussions that the Global Markets Advisory Committee, which I sponsor, raised at our February 13th meeting a couple weeks ago -- global market structure including trading, liquidity, and clearing; global commodity market volatility; and digital assets. I appreciate Commissioner Johnson and the MRAC's recognition and support of the GMAC's work.

It is one of our key traditions that the CFTC's advisory committees have historically complemented one another in order to cover more ground and address the breadth of significant issues facing our markets. Since the GMAC is focused on global business and global markets, including issues that impact strategy and operations, I am glad that the MRAC, which is about risk, can focus on critical areas such as market risk and other risks impacting our market participants, from systemic risk to credit or counterparty risk.

I look forward to hearing today's panel discussions and appreciate that they will help to introduce thorough examination of areas such as DeFi and cybersecurity at the Technology Advisory Committee meeting on March 22nd, sponsored by Commissioner Goldsmith Romero. We just had excellent presentations on electrification and industrial metals markets at the recent Energy and Environmental Markets Advisory Committee meeting on February 28 sponsored by Commissioner Mersinger, and the Agricultural Advisory Committee sponsored by Chairman Behnam will deeply explore geopolitical and sustainability issues on April 5.

As you can see from all of our advisory committees, it is important for the CFTC to have expert advice from market participants and the public. The efforts on this committee help to ensure that the Commission's work reflects input from those directly affected as we consider the most effective and efficient ways to mitigate and manage risk.

Thank you.

MR. FEKRAT: Thank you so much, Commissioner Pham.

So now we'll turn to just a few logistical remarks that I've been asked to mention to committee members.

Please make sure your microphone is on when you speak. The meeting is being simultaneously webcast, and it's important that your microphone is on so that the webcast audience can hear you.

If you would like to be recognized during the discussion, please change the position of your place card so that it's vertically on the table, raise your hand, and Chair Crighton will recognize you and give you the floor. If you're participating virtually and would like to be recognized during the discussion for questions or comments or need technical assistance, please message me within Zoom chat. I will alert Chair Crighton that you would like to speak.

Please identify yourself before speaking and signal when you're done speaking. Please speak directly into the microphone for optimal audio quality on the webcast. Please unmute your Zoom video before you speak and mute after you speak. Please only turn on your camera when you're engaging in discussion. If you are disconnected from Zoom, please close your browser and enter Zoom again using the link previously provided for today's meeting.

Before we begin, we'd like to do a roll call of the members participating virtually so we have your participation and attendance on the record. After I say your name, please indicate that you are present and then mute your line.

James Andrus?

MR. ANDRUS: Present.

MR. FEKRAT: Thank you. Richard Berner? Professor Berner?

(No response.)

MR. FEKRAT: Alessandro Cocco?

MR. COCCO: Present.

MR. FEKRAT: Tim Cuddihy?

MR. CUDDIHY: Present.

MR. FEKRAT: Gina-Gail Fletcher?

MS. FLETCHER: Present.

MR. FEKRAT: Lindsay Hopkins?

MS. HOPKINS: Present.

MR. FEKRAT: David Horner?

MR. HORNER: Present.

MR. FEKRAT: Eileen Kiely?

MS. KIELY: Present.

MR. FEKRAT: Elizabeth Kirby?

MS. KIRBY: Present.

MR. FEKRAT: Craig Messinger?

MR. MESSINGER: Present.

MR. FEKRAT: Jessica Renier?

MS. RENIER: Present.

MR. FEKRAT: Kristin Smith?

(No response.)

MR. FEKRAT: Suzanne Sprague?

(No response.)

MR. FEKRAT: And Professor Berner, you're here. I see you on the screen.

MR. BERNER: Yes, I am. Thank you. I just joined as a panelist.

MR. FEKRAT: Thank you so much. Thank you.

(Pause.)

MR. FEKRAT: I believe Commissioner Mersinger may be on Zoom and ready to speak. If that's accurate, please do so. Thank you so much.

(Pause.)

MR. FEKRAT: So thank you, everybody, for joining virtually. And the Commissioners, thank you so much for your remarks.

We will now hear from Chair Crighton.

CHAIR CRIGHTON: Thank you, Bruce, and good morning, everyone.

Today, as Commissioner Johnson indicated, we will engage in discussions involving cybersecurity matters to be addressed by the CCP Subcommittee, as well as a host of issues relating to the future of finance, climate-related market risks, market structure developments, and interest rate benchmark reforms. All of the topics discussed today are responsive to the

MRAC membership's request for discussion and intended to inform potential MRAC subcommittee workstreams. Particularly with respect to the Future of Finance, Market Structure, and Climate-Related Market Risk Subcommittees, our intention is to finalize membership and leadership roles and establish a pathway for these subcommittees to meet in April.

Looking ahead, I also want to alert our members to our current thinking for future meetings. I anticipate that it would be productive to have an MRAC meeting each quarter this year. Please watch your emails for save the dates.

Now let's turn to the first section of the day, which is cybersecurity and CCP risk and governance. For this section, I would like to introduce Matthew Cronin and Caitlin Clarke, leadership from the Office of the National Cyber Director, to provide opening remarks on matters critical to the nation's cybersecurity strategy.

Matt and Caitlin, if you kindly would, please begin your presentation.

MR. CRONIN: Good morning, everyone.

Commissioners Johnson, Goldsmith Romero, Pham, Chair Crighton, members of the MRAC, colleagues, and friends, thank you so much for inviting ANCD Clarke and I, the Office of National Cyber Director, to this important meeting dealing with a number of pivotal issues.

Now one of those issues is cybersecurity, and it's our understanding that the reason why this topic has come up in this meeting, or at least in part, is based on the recent ransomware attack against ION. That ransomware attack offers a stark reminder to us of the importance of cybersecurity and the importance of third-party resiliency, but I humbly submit that it also reminds us of something far more important. That, ultimately, we are all in this together.

Now I could give a bunch of stats about the importance of cybersecurity, both for the private sector and for society. I imagine you've heard a number of them before. So I'll be brief.

Estimated that the total cost of cyber attacks in 2023 will exceed $8 trillion. That is the equivalent of removing the GDP of California, Texas, New York, and

Illinois off the face of the Earth. That is a monumental risk not just to finance, but to the free world at large.

Moreover, in terms of individual companies, the average cost of a data breach for a company right now is hovering just over $4 million. But again, there is hope. There is a 65.2 percent differential in the cost -- total cost of a cyber attack for companies that engage in rigorous cybersecurity planning and investments and those that do not.

We're all more or less aware of these stats. I won't belabor that point. Instead, I just want to submit to you a different way of looking at this issue, and that is in the historical context. I believe that we are right now at a critical juncture in history. We're between two essential bookends.

The first, as was just mentioned by Commissioner Goldsmith Romero, is the Russian invasion of Ukraine. The second is the potential risk with a Chinese invasion of Taiwan. And what we do in between the years, between this event that's already happened and one that is at the very least has a real risk of happening, will be of utmost importance.

We've already seen the threat and the harm caused by Russian ransomware actors and Russian APT groups, and we are starting to see the increased risks that they may pose as whatever chains are fettering them down are loosened as the struggle becomes more and more desperate for the Russians. And again, as a matter of public record, the potential invasion of Taiwan, CIA Director Burns has stated publicly as a matter of intelligence, the United States is aware that Chairman Xi has instructed his military to prepare for a military invasion of Taiwan no later than 2027.

Moreover, Assistant Director Easterly stated not less than 2 weeks ago that if that were to occur, there is a very real risk the Chinese would engage in cyber attacks against U.S. critical infrastructure. We can all imagine the sort of devastation that that could cause.

So we are in the middle of that bookend now, and every decision that we make -- on the individual level, the corporate level, the government and nationwide level -- will make a dramatic difference in the future to ensure the continued prosperity and safety of, again, the private sector, individuals, and ultimately the American people. So every step of the way, including today in this meeting, we should be asking ourselves what can we do to ensure not only the safety, not only the security, but that resiliency?

As part of that effort, the Office of National Cyber Director recently -- and the Biden administration has recently unveiled the National Cybersecurity Strategy, and I'll have ANCD Clarke provide more details what we plan to do to achieve those ends through this strategy.

MS. CLARKE: Thanks, Matt, and thanks, everyone, for having us here today.

As Matt said, last Thursday, the administration released its National Cybersecurity Strategy. It is building upon the work that we have all done over the last 10, 20 years. I would say it's an evolution, not a revolution. We've had a lot of work in this space, and looking around this room, as folks who have really focused in on cyber risk management for years.

The strategy really is based on two fundamental shifts. First, that we rebalance the responsibility to defend cyberspace. For years, we've had a focus on awareness. "Don't click on that link. Be careful. Everyone watch out."

I don't know how many of you all have had the phishing training in your organizations and really hope that nobody clicks on that link about "Let's fill out that March Madness bracket next week." That is not a sustainable strategy given the risks that Matt laid out for us.

So we need to fundamentally rebuild our cyber ecosystem to be more secure and resilient and transfer the risk from individuals, like my mother who I have to tell, "No, your bank would never send you that message. Do not answer that, or do not click on that," from small businesses who bear the burden of these ransomware attacks and local governments who bear this burden, to the larger, more capable, and more resourced actors in cyberspace. So that is a first shift in the strategy.

The second is to focus on long-term investment. So when we are faced with making a decision about something that is quick and easy and will address the risk that we're facing right now versus a long-term investment in security and resilience, that people choose the latter. Quick fixes may work now, but it's not going to protect us in the long run in the environment that Matt just laid out. That our adversaries are continually looking for ways in, and if we don't start to get out in front of them and start thinking more strategically, we will continue to be on the defense.

So our strategy is out now. It is one based in partnership. So I'm looking around this room. We all have a role to play in implementing the strategy. It is bold. It is not something that is going to come into play in the next weeks or months. It's going to take years for us to implement all of the goals and achieve the vision that we've laid out in the strategy.

But we feel it's important that we lay out our vision, that we start to move in a different direction -- sorry, not a different direction, but a more thoughtful direction about where we are going in terms of, looking around this room, regulation in places other than the financial sector and investments in our future. We think cybersecurity should be at the forefront of every discussion when we've got new infrastructure being built, a clean, green economy. Cybersecurity should be at the forefront of those conversations.

So I encourage you all to read the strategy, and I appreciate you all for having us here today, and I'm going to turn it over to Matt to just kind of put a ribbon on what we're thinking about in the Office of National Cyber Director.

MR. CRONIN: Thank you, Caitlin.

And when we were discussing earlier how to close this out, I realized that I may have been a bit of a downer in the first part. And so I'm going to end with a message of hope.

So first part was the stakes that we all have right now we're sharing together, how we're going to get out of this, how we're going to fix it through the strategy, and then, finally, as a kind of a coda, a message of hope. And I want to remind all of you what happened just a little over a year ago in Ukraine.

So the last time the Russians attacked Ukraine, they turned out the lights quickly using a cyber attack. And then, little over a year ago, when the Russians invaded Ukraine again and went all out, they had the same elite cyber warriors went to the electrical system, the electrical infrastructure in Ukraine, with a goal of turning off the lights. And they thought they were going to do what they did last time, which is go after the smallest, weakest member, disable them, and then keep going from there up the system.

So they went. And then, speaking in generalities, they thought, well, we'll just take out this -- we'll blow out this one person, this one substation. What did they found out? Well, they found out we're not just going after this one person. That entire station is working tirelessly to keep us out.

It's not just that one station. The entire Ukrainian electrical grid is working tirelessly to defend their system. Not just that electrical grid, it's the entire nation of Ukraine united. And not just the nation of Ukraine, it was the United States and its allies providing key intelligence. And not just the United States, NATO, EU, it was also the private sector -- Microsoft, Mandiant, and others -- filling the gaps.

And for the first time potentially in human history, cyber defense was exponentially stronger than cyber offense, and it has remained so to this day in Ukraine, to the point they have to use what is now at this point precious few munitions that the Russians have left to turn off the lights.

We need to turn that instance into our continued reality across the free world. That is the recipe for success. We are all in this together. And when and if we work together to achieve that goal, we will have a safe and secure and resilient cyber future.

Thank you.

CHAIR CRIGHTON: Thanks. Thanks very much, Matt and Caitlin.

Now we'll turn to the first panel of the day, which will consider leadership perspectives in the area of resilience, recovery, and cybersecurity risks. First, we'll hear from Walt Lukken, President and Chief Executive Officer of the Futures Industry

Association. Then we'll hear from Tom Sexton, President and Chief Executive Officer of the National Futures Association. Finally, we'll hear from Julie Holzrichter, Chief Operating Officer of CME Group.

I'd like to ask Walt to kindly begin the presentation.

MR. LUKKEN: Thank you, Chair Crighton, Commissioner Johnson, and fellow commissioners. It's an honor to be here to talk about this important issue regarding the ION recent cyber incident.

In the early morning hours of Tuesday, January 31st London Time, FIA became aware of an outage at ION Markets impacting the trading and clearing of the exchange-traded derivatives world. FIA immediately began working with our members to identify the scope of the outage to assess the potential impact on our markets.

ION is a software service provider that offers middle and back-office products to clearing firms that are active in futures markets around the globe. Now these services are embedded in the execution and clearing workflow of our market participants in our industry.

Now while the number of clearing firms that use ION's suite of clearing products is limited, the interconnectedness of our markets made the outage impactful through the entirety of our marketplace. By roughly 7:30 a.m. Eastern Standard Time, it was clear that the outage was significant for affected firms. We also heard the first rumblings that this was not simply an outage, but possibly a cyber incident.

Later that morning, FIA held a call with roughly 150 industry members from the Americas, Europe, and Asia. We held three additional calls with members that first day, including those in the Asia-Pacific region. Also on that initial day, FIA contacted the CFTC and NFA to share what we had learned and to highlight some potential regulatory challenges.

These three-a-day calls in the first week of the cyber attack, which grew to 700 attendees, were critical to ensure the important information around the cyber attack were being shared with market participants.

On Monday, February 6th, nearly a week after the initial outage, our industry began the reconnection phase of the incident after ION accelerated the recovery and rebuilding of their systems over the weekend. To assist firms with this stage of the recovery process, FIA continued to have ad hoc calls and share industry protocols and best practices around reconnection. By the end of the second week of the incident, it is our understanding that most firms utilizing ION's suite of products were back to business as usual operations.

With this timeline as background, I'd like to share some initial observations. First, the importance of flexibility and communication during a crisis cannot be overstated. We were quickly able to centralize information, dispel rumors, and share practical experience.

Exchanges and clearinghouses from around the globe deserve a lot of credit for their response. They were flexible in extending deadlines, giving firms more time to recover data, keeping clearing windows open, and providing confidence that markets would continue to function.

Human judgment and experience are critical to risk management, and we saw it on full display during that recent episode. The Commission and NFA also should be commended for their direct engagement with market participants and the flexibility afforded to some of the reporting requirements for registered entities. These reduced stress without adding risk when the markets were most vulnerable.

Today, FIA is announcing the formation of a Global Cyber Risk Task Force to look at the ION event and to develop recommendations for improvements to our markets. This task force will focus on areas including existing cyber protections and protocols, the effectiveness of the industry's initial response, best practices around reconnection, and safeguards around third-party service providers. We aim to release an initial report by the end of the second quarter this year.

Additionally, resilience requires practice, and business continuity testing is crucial to helping derivatives firms prepare for unplanned market disruptions. Since 2004, FIA has hosted an annual disaster recovery exercise for market participants from around the globe. With a new lens towards the events at ION, FIA is reviewing how we conduct this annual exercise.

FIA also recommends simulated exercise held by public authorities aimed at improving responses to a range of cyber threat scenarios within the financial sector. The CFTC has held such events in the past. I know Julie and I participated in the Hamilton exercise a few years ago, and we recommend doing such regular exercises in the future.

FIA is committed to working with the CFTC, NFA, and the broader derivatives industry to ensure our markets are resilient against cyber threats.

Thank you again for this invitation to discuss these important matters.

MR. SEXTON: Good morning, and thank you, Commissioner Johnson and Chair Crighton, for inviting NFA to present views today with regard to the ION incident.

Good morning also to Commissioners Pham and Goldsmith Romero.

The ION Markets cybersecurity incident, which caused a significant outage, highlighted the risks associated both with cyber incidents and third-party service providers. In the aftermath of this incident, we believe it serves as one more example of the resiliency of the derivatives industry.

I commend my industry colleagues on this panel and U.S. exchanges and clearinghouses that worked extensively and around the clock with market participants to mitigate this incident's impact. FIA, as Walt indicated, held multiple daily coordination calls to share critical credible information, and its willingness to allow NFA and other regulators to participate on those calls allowed us to understand the gravity of this incident and work with the CFTC and CME Group to provide prompt flexibility to U.S. FCMs in terms of their regulatory and reporting obligations.

The CFTC also deserves credit for engaging promptly with market participants and the industry's SROs to evaluate this incident and mitigate its impact.

The incident raises important questions. There are several. Can we further safeguard against these incidents in the future, and in the event they occur -- and they may despite the safeguards -- what more can we do to effectively respond?

In evaluating these questions, we should all recognize that our member firms have adopted robust safeguards already that need to be adapted in light of today's and tomorrow's ongoing challenges and threats. NFA, the CFTC, and the industry have worked together to adopt a number of measures applicable to our member firms and relevant to the ION incident. Post 9/11, in 2003, we adopted a compliance rule and interpretive notice requiring our members to adopt business continuity and disaster recovery plans.

As technology and cyber threats continued to evolve and advance in sophistication, in 2015, we adopted further guidance, pursuant to our supervision role, requiring our members to diligently supervise the risk of unauthorized access to or attack upon their information system technologies.

Last, in 2021, NFA required member firms to adopt supervisory frameworks relating to third-party service providers that perform regulatory functions to assist our members in fulfilling their regulatory obligations. Two points about this notice. Number one, it recognizes that these providers are a benefit to our members, but they also present risk. The requirements generally follow best practices for vendor management, perform an initial risk assessment, perform onboarding due diligence, monitor the providers, have termination practices and mutual recordkeeping requirements.

Second, we believe that in adopting this, after the CFTC approved it, the CFTC and NFA became one of the first among the financial industry -- within the financial industry sector to adopt these types of supervisory requirements with regard to third-party service providers and proactively address the risks associated with these providers in order to mitigate them.

In conclusion, as very concerning as this incident was, we should learn and benefit from it. NFA is committed to work with CFTC, FIA, CME, ICE, and other industry participants to determine what, if any, changes should be made to our current requirements in the areas of cybersecurity and third-party service providers. We must continue to engage as an industry in annual disaster recovery exercises and do so, if possible, as part of a U.S. financial sector.

Last, we should recognize that we are part of an industry that places a high value upon coordination among market participants and with regulators, which is critical to addressing successfully these types of disruptive events in the future.

Thank you.

MS. HOLZRICHTER: Commissioner Johnson and fellow commissioners, I'd like to thank you for having this discussion today on such an important topic and for inviting me to speak on behalf of CME Group.

As with all businesses, cybersecurity and risk management are top of mind daily at CME Group. We are constantly working to remain vigilant against attacks and any disruptions. When it comes to cyber events, it is often said that it is not a question of "if," but "when." The ION ransomware incident is a reminder of the importance of cybersecurity and risk management and the reason we work hard as an industry to put in place the procedures and protections we have in our markets.

The event is a testament to how the industry -- clearinghouses, FCMs, and regulators -- worked together to support a resilient and safe system. I know I echo much of what Walt and Tom have already said, but it warrants being restated. The industry coordination in this case did not occur by happenstance. We have always taken a proactive approach and engaged in the sector discussions to help drive the risk mitigation priorities facing our industry.

Beyond our routine points of engagement, we relied on lessons learned from industry exercises and collaboration fostered through public and private information-sharing groups over the last decade. These engagements helped to strengthen our collective muscle memory for when the real-world scenario occurred.

Let me focus specifically on the steps we took at CME. The ION ransomware event impacted a subset of FCMs, with a material impact for an even smaller subset therein. At CME, fewer than 20 percent of our clearing member firms were impacted.

As the events around ION unfolded, CME Group took its market structural role and clearinghouse role very seriously, immediately relying on the frameworks we have in place to address such an incident. We're really proud of the work our teams did to support our impacted FCMs.

We became aware of the event as a result of our systems monitoring practices, as we observed an unusual buildup of message queuing. We quickly took steps to ensure our environments were protected, including blocking network connections with ION, evaluating our environment for the published indicators of compromise, reviewing our own systems that we believed could be exposed to contagion risk for any potential vulnerabilities, and working to validate what we were seeing and our understanding of the ransomware attack against ION.

As I previously noted, a limited number of clearing members were impacted at CME Group. Shortly after becoming aware of the ION incident, we engaged with firms to help them retrieve necessary files and perform functions within our own systems. We worked with the impacted clearing firms to extend our end-of-day processing timelines to allow firms extra time to complete their tasks. We issued a notice to our clearing firms that reporting may be delayed. We also engaged in industry discussions to ensure priorities and challenges were being highlighted.

As firms were impacted differently, we worked with them to assist in their recovery once the new environments had been built. In addition, with respect to risk management, it's worth noting that we put in place enhanced risk monitoring for the impacted firms. Some of the impacted clearing members were not able to submit customer gross margin files, so we leveraged our own records and knowledge of relationships between the gross and net margin requirements to track ION's customers' gross margin requirements, making adjustments to the impacted firms' requirements as appropriate.

As we know, and this incident reaffirmed, collaboration across the industry is critical when there has been a cyber event, as well as in advance when plans can be developed, tested, and verified. When there is an issue, there are essential best practices to be followed, including timely information sharing through various industry groups, including direct CISO-to-CISO conversations across all CCPs, clearing members, and vendors; sharing information about indicators of compromise, threats, tactics, et cetera; and coordination on reconnection frameworks, which was drafted as an outcome of a Hamilton exercise as an example of the public and private sector collaboration I noted at the start of my remarks.

Third-party risk management is a growing and evolving field. Through a combination of due diligence, strong contract terms, ongoing monitoring and assessments, and good incident notification and communication protocols, we believe risks introduced by using third parties can be addressed and managed. I believe today's dialogue and ongoing due diligence by the industry demonstrate a commitment to ensuring this risk mitigation continues going forward.

In closing, I'd like to acknowledge and thank the Commission for today's discussion and the agency's efforts and collaboration with the industry as we worked through the events of the ION compromise.

Thank you.

CHAIR CRIGHTON: Thanks very much, Walt, Tom, and Julie.

Now for the second panel of this section, we'll hear regulatory perspectives on the matters discussed. First, we'll hear from Amanda Olear, Director of the CFTC's Market Participants Division. Then next, we'll hear a presentation from Greg Ruppert, Executive Vice President, Member Supervision for FINRA.

MS. OLEAR: Thank you, Chair Crighton, and thank you to Commissioner Johnson, the Commission, and the MRAC as a whole for the invitation to speak with you today.

To echo the remarks of Chairman Behnam just last month at the ABA Derivatives Conference and in keeping with some of the themes that Walt, Tom, and Julie just spoke about, MPD is acutely aware that we are in a time where our registrants are now facing a broad array of challenges to their risk management activities, ranging from geopolitical events like the ongoing conflict in the Ukraine, public health crises like pandemics, and macroeconomic forces such as shifts in monetary and fiscal policy to threats of operational disruptions, which are amplified by an increased reliance on technology and the ever-evolving sophistication of cyber criminals.

Given these challenges, MPD believes that there may be a need to update the tools, resources, and rules regarding the management of risk. Good governance requires a comprehensive commitment to achieve the goal across all players in the system. And like the chairman and the Commission, I believe that the Commission plays a critical role in fostering such a culture across all of our registrants and registered entities.

Accordingly, MPD is embarking on an effort to revisit its risk management requirements for FCMs and swap dealers to determine whether there is space to better adapt them to meet these current and evolving challenges. As part of this effort, as noted in the Commission's Unified Agenda, the Commission will be issuing an Advance Notice of Proposed Rulemaking posing specific questions soliciting feedback from the public to inform our work in this area.

Additionally, MPD plans to begin engaging directly with our registrants to get their perspectives on our risk management regime and to identify opportunities to enhance its effectiveness for identifying, monitoring, and managing all of the attendant risks to their FCM or swap dealer activities. A core focus of those discussions will be identifying key risk areas that should be monitored and managed, amendments to periodic risk reporting, and risk management governance more broadly.

A key risk area that I'm sure is at the forefront of everyone's minds is cyber risk, including both how to mitigate it and how to recover from a direct cyber attack or one on a third-party service provider. Although our registrants are generally subject to cybersecurity requirements, whether from the NFA or through prudential or other regulatory regimes, MPD believes the Commission could play a more direct role in fostering strong operational resilience practices amongst our registrants.

At the Commission's request, MPD has begun work to develop policy recommendations addressing FCMs and swap dealers with respect to their cybersecurity practices. It is my hope that this workstream will serve to enhance the Commission's regulatory oversight of our registrants to ensure the continued protection of customer and counterparty information and assets.

Especially given the ever-evolving nature of cyber risk, I am aligned with Chairman Behnam in the belief that by establishing thoughtful, tailored, and adaptive CFTC-specific cyber requirements for FCMs and swap dealers and continuing our deep engagement with our registrants to ensure their continued compliance with them, the CFTC can help raise standards in a way that will ultimately improve operational resilience across the financial sector and serve to better protect the markets and their participants.

We look forward to engagement with the public on these topics in the coming months.

Thank you.

CHAIR CRIGHTON: Thanks, Amanda. Greg, we'll turn to you.

MR. RUPPERT: Great. Thank you, Chair Crighton, and thank you, Commissioner Johnson, for including us in this very important discussion today.

Just real briefly, I know most of you, given your familiarity with the CFTC and our partner or our connected SRO, the NFA, I just wanted to briefly talk about FINRA and how we're established. We're a statutorily authorized SRO as well. We oversee the U.S. broker-dealer industry and the registered representatives, and our mission is squarely to protect investors and safeguard market integrity.

In this regard, we oversee over 3,400 broker-dealers and over 624,000 brokers across the country. And not only do we conduct thousands of examinations a year as well as investigations, but also analyze nearly billions of daily market events that come through.

We're actively engaged in providing essential tools for not only our member firms, but also investors as well as policymakers as we address various risks and assess threats that are coming. And today's discussion I think is a perfect example of how we need to be proactive and not reactive, especially in the cyber arena.

When I look back at my time in the government, specifically working in FBI Cyber, as well as in a leadership role at a major broker-dealer, cyber has continued to become increasingly complex, and we're seeing more threat actors enter the space that was predominantly reserved for other areas of the financial industry. But we're seeing the specialized knowledge and complexity that is hitting our shores on a daily basis.

So, today, I thought I would talk a little bit about the top cyber threats facing the financial industry, business continuity planning, as well as how FINRA envisions emerging technologies and tradition market participants and how we look at the supervision to include other areas such as digital assets and the FinTech-related aspects of our business.

When we look at our cybersecurity oversight, we clearly see cybersecurity remaining a key operational risk factor, one so much that we've actually separated out cybersecurity risk and technology risk out of our traditional operational risk category and are handling this as a separate category. We're looking to educate our members from our small firms to our large broker-dealers to be more capable of assessing this threat and dealing with the challenges that we're all facing as an industry. We're also looking at expanding our capabilities to interact with threat intelligence from across the U.S. Government as well as other entities that are clearly in this space and be able to bring that forward to our membership to make them more knowledgeable in this area and, again, more proactive in their ability to assess those threats.

We've created a Cyber and Analytics Unit, and we've actually broken out additional teams related specifically to cybersecurity, cyber fraud, which we also refer to as computer-enabled fraudulent activity, that's impacting our firms as well as their clients, as well as a crypto asset investigations unit.

We also regularly alert our membership and others to cyber threats that we're identifying. We do that through our public channels as well as our private portals. We're also looking to connect our membership with the cyber threat and cyber risk experts within the United States Government, with deeper dive discussions related to those activities. And then we also have our teams that are examining firms for their compliance with federal security laws and regulations as well as their approach to cybersecurity risk management, as well as conduct investigations related to cyber-specific misconduct that we're seeing.

Turning briefly to how we see cybersecurity threats and the top challenges. Our broker-dealers are required to develop reasonably designed cybersecurity programs and controls consistent with their risk profiles, business models, as well as the scale of their operations.

Our focus is also to ensure that we have impact addressing the following top risk areas. Some of those have already been talked about at length today, but from our perspective, we're seeing phishing obviously being one of the key vectors of attack. We're also seeing the smishing-related attacks that are impacting specifically in the broker-dealer space, and we saw a significant uptick related to the pandemic and a shift from an in-person environment to more virtual environments from not only their coverage, but also their interaction and engagement with their clients, some of which tend to be the greatest risk profiles that we see being targeted by threat actors.

Ransomware has continued, and we have seen it increase but also not only in frequency, but we're looking also at the profitability to suggest future risks that are going to continue on that front. We've seen addition in terms of the ransomware as a service, allowing for a greater ability to use it across various threat actors and as well as criminal groups.

We recently published a regulatory notice at the end of last year, our Regulatory Notice 22-29, alerting firms to increase ransomware risk. So we're doing our part to educate and provide specific action steps firms should be on the lookout for as we see these threats come through not only other industries, but also our industry and as they trickle down through larger entities into even the smaller entities.

Supply chain attacks are definitely an area where we're seeing and I think we'll discuss today on the various incidents that have happened. We called that out back in 2021 towards the end of the year, reminding firms about their supervisory obligations to their outsourcing and third-party vendors, and we'll continue to provide notification, insights, as well as coverage related to this key area.

One that we're also turning a significant amount of attention to this year is the threats related to what the industry calls kind of at large is the "insider threat." Why we're of heightened concern related to this area is that the attacks we think might become more prevalent related to industry-wide reductions in staff as well as decreases in financial compensation.

When those items capture the headlines, I think it's key for us to also call out to our member firms that their workforce is also a potential area of vulnerability or risk, and the insider threat, often reserved for other critical infrastructure sectors, is something that is very important for the financial service sector. And we've assessed, and we have actually seen instances where the insider threat risk has actually caused significant damage. That damage can impact not only markets, but it can impact their investors as well as other aspects of the business.

As firms move towards more hybrid and remote environments, a shift in their supervisory controls as well as their risk focus should also cover these areas. As well as when we're seeing a high demand for specialized staff, a kind of renewed vigilance in terms of doing the due diligence -- background checks and other areas -- of bringing on new staff is something that we should always keep at the front of our minds in assessing these kind of areas.

We've called out areas such as financial loss, reputational risk, and operational failures in a host of FINRA rules as well as SEC rules that require firms to focus specific attention on it.

Another area that is definitely one that's seen in our focus is the social engineering attacks, and the increase not only in frequency, but also complexity. As most of you know that are in this area, it's one of the key areas for human engagement in terms of 95 percent of cybersecurity areas being traced back to human error or, as was discussed in one of the earlier presentations, the phishing attacks and the complexity of trying to ensure your employee base as well as your client base doesn't subject themselves to giving away passwords or introducing malware into systems through clicking on links or falling to the social engineering.

The rise and engagement of people on social media sites as well as the constant drumbeat related to successful intrusion attacks really are creating a perfect storm of the amount of available data to outside threat actors, connected with what we're willingly and voluntarily putting on about ourselves, really adding to the vulnerability for social engineering. The increase and rise of AI or machine learning technologies, such as ChatGPT, key areas that will help facilitate the threat actors to engage in this space.

We've actively covered this in our 2023 report where we've highlighted not only from our exams, but also additional risk identification areas. We've particularly highlighted the risk of social engineering, which is also available on our website.

I'll touch really quickly on the business continuity plans. That is something that we are reinforcing with our membership. The ability to be resilient in this space, to have backups and be able to operate also in virtual environments is going to be key that we're looking at from a risk perspective.

And then as we move on to not only just new technologies, new business models, but new areas of coverage such as the digital asset and crypto securities area is something that will continue to be at the forefront of what we're tracking and watching and partnering with other key agencies in order to be ready to address that situation. We're conducting surveys within our membership. And in 2020, our initial outreach resulted in seeing about 20 of our member firms reporting in to us that they had some nexus to digital asset-related businesses, whether it's directly or through their affiliates or their employees with outside business activities.

What we saw in a recent survey we did last year was an additional 200 firms that had some level of nexus to this space. So a significant increase, and we only expect that to grow. So we are actively engaged in advising of the threats and actively investigating any related fraud or fraudulent-related activity that's occurring at, by, or through our member firms in these spaces.

So I'll pause now and thank you again for including us in this discussion. I think it's valuable for all of us to work collaboratively together across the various private sector as well as quasi-Government and Government entities. We do know that the threat actors are collaborating on the dark web, and it's incumbent upon us to be able to meet that threat as a unified, one team approach.

CHAIR CRIGHTON: Great. Thanks very much, Greg. We appreciate you and Amanda.

We'll turn now to the third panel of this section, which relates directly to our CCP Risk and Governance Subcommittee. This subcommittee met last week and had a very productive discussion concerning current and anticipated workstreams.

First, we'll hear from Ashwini Panse of ICE, who will focus on the subcommittee's work, including with respect to forward-looking workstreams. Then we'll hear from Suyash Paliwal, Director, and Kirsten Robbins, senior special counsel, in the CFTC's Office of International Affairs.

After these perspectives, we'll have some time for open discussion from our members. Ashwini?

MS. PANSE: Thank you, Chair Crighton and Commissioner Johnson, for the opportunity to speak here on behalf of ICE.

Allow me to begin by saying that we would have thought that as we emerged out of the COVID-19 pandemic and reopened our economies that would have been enough stress for the markets to have worked hard to absorb. But add another layer on top of that, a war in Europe, where the aggressor is the main energy supplier to the continent, you have the recipe for a very volatile market.

We have also witnessed the energy and the political pressure increasing on the energy trilemma. And these are only some of the factors that the markets have been seeking to absorb.

If we step back as our industry rose to face these new challenges, the past year has also reinforced longstanding truths about the strength of our markets. With uncertainty all around us, risk management and price discovery are more important than ever.

The futures markets exist to do two main functions. The first is to help our customers to manage risk, and the second is to provide pricing that is critical to the efficient allocation of capital. It is important to have a steady stream of prices to support investment decisions out into the future.

When we look at the markets that ICE supports, we have seen a number of disruptions over the last year. 2022 stands unique in the breadth and extent of risk management that many of our customers have had to deal with, and the reality is that they have dealt with it extremely well. The system that we have built since the 2008 financial crisis has stood largely very well through the year of crisis that we have had.

Just to give you an example, in the natural gas market, the price on TTF went up tenfold from the middle of 2021 to the end of 2022, briefly touching more than 300 euros for megawatt hour in the third quarter of 2022. That was a significant stress on the market and particularly driven by Europe seeking to fill its storage capacity in the third quarter last year leading up to winter.

What we have seen since then is that those prices have come down. We're now sitting under 55 euros per megawatt hour for TTF, and a lot of that is driven by the fact that the weather has been unseasonably warm in Europe, storage capacity is filled to higher levels, renewable energy is higher at this point in the year, and there is an increase in regasification capacity that's been brought onstream in Europe.

It's quite unclear what the impact on the prices will be as we approach the next winter, but Europe has certainly been in a much stronger position now than it has been prior to the crisis.

The key thing for this group to take into account is we ended the year in 2022 with the highest number of participants in the market ever. That's after all the market stress we talked about. The risk that was managed by that market was at its highest level, and again, the whole market infrastructure around that market was 100 percent robust and managed its way through that risk incredibly.

We have seen a rather unhelpful implementation of price caps in the futures market in Europe. It is well publicized that ECB, ESMA, and ACER, as the regulatory bodies in Europe, all disagree with that implementation. We certainly don't see that that's going to have any positive impact in the market.

It goes without saying that despite the current economic environment being particularly challenging for financial stability and the risk being fragmented, net net, the industry has done extremely well to manage through the crisis. As we've seen new shocks emerge, forums, such as the MRAC and its subcommittees, are critically important and useful for stakeholders in cleared markets to come together to discuss areas of interest, gather input on a variety of regulatory and market issues that affect the integrity and competitiveness of derivatives markets, and to provide recommendations with a focus on the stability of the broader financial system. We should continue to advocate for a global regulatory system that is coherent across the different jurisdictions, with deference to local authorities where that makes sense.

The CCP Risk and Governance Subcommittee met last week to reexamine the current and potential workstreams in light of recent unprecedented volatility in the commodity markets. I wanted to take a couple of minutes to acknowledge the work completed by the subcommittee as a part of the current workstreams under the leadership of subcommittee co-chairs Lee Betsill and Alicia Crighton.

Members successfully worked together to publish two papers on CCP margin methodology and CCP governance at the February 2021 MRAC meeting. And two additional papers on CCP capital skin in the game and CCP liquidity and stress testing were presented at the July 13, 2021, MRAC meeting.

The reports provide a great summary of what was discussed, noting that our policy views were aligned as well as noting policy views where agreement could not be reached between market participants and CCPs.

With respect to the CCP governance discussion paper, the subcommittee provided recommendations and in some instances proposed rule text. In August 2022, the Commission proposed several amendments to the

Commission Regulation 3924 that are consistent with subcommittee's recommendation to enhance the Commission's DCO governance standards. The Commission is now drafting the final rule. The subcommittee is hopeful that it can continue to provide similar useful insight and analysis to aid in the Commission's work.

The margin methodologies discussion paper reflects the collective work of the subcommittee in putting forth recommendations to the CFTC in the following key six element areas of a robust margin framework -- anti-procyclicality, concentration and liquidity add-ons, intraday and ad hoc margin calls, margin period of risk, pricing, and transparency. Many of the recommendations are already being followed by the CCPs today.

To the extent where areas of consideration lacked agreement, the subcommittee will explore if additional consensus can be accomplished.

The CCP capital and skin in the game and CCP liquidity and stress testing papers identified topics on which the subcommittee agreed and disagreed. However, the papers did not make any specific recommendations to the MRAC. There was a broad agreement in the subcommittee that stress testing is a critical element to ensure the resilience of DCOs and the financial system.

As such, many of the practices for stress testing by DCOs identified by the subcommittee are practices that are already employed by the DCOs today, particularly by the systemically important DCOs, SIDCOs, and those electing to be Subpart C DCOs. These broad areas of agreement reflect the principles for financial market infrastructure. The areas of agreement noted in both the papers demonstrate a healthy coherence on unbiased risk management practices that are already employed by the DCOs. These practices allow DCOs to continue to follow the regulatory mandate of prioritizing the safety of the markets and successfully navigate market stress events in the future.

I'd like to also take a minute to also add the good work and progress we, as an industry, continue to make on the topic of transparency as CCP12, the global association of CCPs, continues to partner with SIFMA

AMG and FIA. As a group of CCPs, we recognize the importance of operating highly transparent CCPs and believe transparency is critical to supporting healthy derivatives markets.

On that line, coming from this industry partnership, the disclosures CCPs make today and transparency CCPs provide today is even more enhanced with public quantitative disclosures now available 1 month earlier from first quarter of 2022 and onwards. Some of the CCPs today also offer quarterly disclosure calls where market participants are invited to listen to qualitative commentaries that CCPs offer and our market risk and market development products CCPs offer for clearing.

To the extent where areas of consideration lacked agreement, as we move forward in 2023, the subcommittee will explore if additional consensus can be accomplished and a dialogue opened, especially in the light of recent events and continued geopolitical tensions involving major commodity-producing countries and heightened macroeconomic uncertainty in an environment of tightening financial conditions.

Just to name a few areas of focus discussed, they already aligned with workstreams identified and are undertaken by global financial center regulators. To give a few examples, these may include price and volatility controls in light of the LME event, liquidity preparedness of market participants in the event of another bout of extreme market volatility, responsiveness of margin models to market stresses, opacity of commodity markets and data gaps in regulatory reporting, transparency in centrally cleared and uncleared markets, variation margin processes, and recovery and resolution.

In closing, I would like to add that the subcommittee also discussed merits of an open dialogue with other advisory subcommittees on overlapping topics like market structure, cyber risks, and new technologies. I look forward to a productive 2023 and would like to thank the chair and the Commissioner Johnson for the opportunity to speak here.

Thank you.

CHAIR CRIGHTON: Thanks, Ashwini. Suyash?

MR. PALIWAL: Thank you, Commissioner Johnson, Chair Crighton, and members of the MRAC for this opportunity to speak. I and my colleague Kirsten Robbins will speak briefly about some international work on the topic of derivatives margins.

In the wake of the volatility caused by the onset of the pandemic, IOSCO, CPMI, and the Basel Committee established a joint group to consider the dynamics and liquidity effects of margin by looking at the market dynamics during that period of time, particularly March 2020. CFTC co-chairs this work with the Bank of England.

A report was published in September of last year, summarizing data collected and many detailed comments received from industry and other stakeholders. We generally think of this report and the work undertaken to generate it as Phase 1 of the project.

Broadly, the observation of Phase 1 was that the clearing ecosystem and margin in both cleared and uncleared markets functioned as designed, but the size of the calls was still high, and it is the benefit for the system for there to be greater preparedness among market participants. This could mean greater transparency by those issuing margin calls, measures that market participants could take to enhance preparedness, and a clear understanding of the responsiveness of margin to market volatility and price levels.

The report proposed further policy work in six areas of focus, and there is some overlap with what Ashwini just covered for the subcommittee. This progression from empirics to policy considerations we generally think of as Phase 2.

In the interest of brevity, I will hand over the floor now to Kirsten Robbins from the Office of International Affairs for some further details about Phase 2 and its six areas for follow-up work. I note that she is co-chair of CPMI-IOSCO's Policy Standing Group, so brings a highly knowledgeable perspective on this work.

Kirsten, the floor is yours.

MS. ROBBINS: Thank you, Commissioner Johnson, Chair Crighton, and MRAC members.

So I'll pick up with the six areas of follow-up work. The Joint IOSCO-CPMI-BCBS Group is handling two of them. That's enhancing the transparency of cleared initial margin at various levels of the clearing ecosystem. They're also looking at exploring the use of metrics and other tools to identify baseline expectations of procyclicality in cleared markets and to address, among other things, the responsiveness of initial margin models to market stress.

CPMI-IOSCO, through the Policy Standing Group that I co-chair, is considering streamlining of variation margin practices in cleared markets, and this includes considerations of intraday margin call practices.

Then the IOSCO-BCBS Working Group on Margin Requirements, which is co-chaired by Rafael Martinez of the Market Participants Division, is looking at two issues regarding noncleared markets, examining the responsiveness of initial margin models and streamlining variation margin processes in the noncleared markets.

And then, finally, the Financial Stability Board is engaged in work to consider recommendations to enhance the liquidity preparedness of market participants, as well as data gaps in regulatory reporting.

Given overlap and interaction among these topics, there is significant effort to coordinate among the groups. And as we do the policy work, we know that liquidity is one objective, but not the sole objective of ensuring its financial stability, and it's really critical that we do not undermine the G20 reforms on central clearing in response to problems that were not ultimately caused by the CCPs in March of 2020.

We also want to ground the Phase 2 work in data, as we did with Phase 1, and consider the costs, benefits, and other challenges of various policy proposals. It's really complex work, and there's quite a bit of it. So you will be hearing more over the course of this year about our project. There may not be simple answers to all of these follow-up issues, but we do really have a good group of experts engaged, and they're quite optimistic.

And specifically here at the CFTC, we've committed significant staff resources across both phases of this work. This is an interdivisional office team taking several leadership roles in many of the projects and the participating groups from the Division of Clearing and Risk, Market Participants Division, and the Office of International Affairs.

Thank you.

CHAIR CRIGHTON: Great. Thanks very much, Ashwini, Suyash, and Kirsten.

We'll now hear policy remarks from Chris Hayward, Chairman of Policy and Resources from the City of London Corporation, to open the second section of today's meeting.

MR. HAYWARD: (on recording) Members of the Market Risk Advisory Committee at the CFTC, I'd like to thank you for the honor of addressing you today, and I offer my apologies that I cannot be with you in person. I have huge personal admiration for Commissioner Johnson and congratulate her on today's really positive initiative.

As policy chairman of the City of London Corporation, I have the privilege of serving as de facto political leader of the organization which represents the United Kingdom's financial and professional services sector at home and abroad. We, at the City Corporation, value our transatlantic Anglo-American relationship deeply, and we are committed to engaging with U.S. stakeholders, which is why I'm so grateful for today's opportunity.

Though our partnership excels in many areas, few are as strong, as fundamental, or as mutually beneficial as financial and professional services. The United States was the UK's single largest trading partner in 2022, accounting for 16 percent of total UK trade, of which financial services trade totaled 28.6 billion pounds.

We see the United Kingdom and the United States as the world's two leading financial centers, having a shared interest in working together to address issues affecting the sector. Areas such as innovation in digital assets, central bank digital currencies, and voluntary carbon markets are all ripe for closer collaboration and regulatory alignment.

We believe that working together, we could provide leadership on the international stage. We can set standards, reduce costs and burdens on businesses, and ultimately deliver tangible policy returns to help our financial sectors thrive.

Critical to achieving closer alignment between our two nations will be the Financial Regulatory Working Group. It is our hope that this group will become the long-term mechanism for coordinating regulation, aligning our international approaches, and allowing interoperability.

The work of the British American Financial Alliance will also be important, allowing industry to contribute, ensuring that voices at the cutting edge are heard. Because ultimately we know that technologies, whether in cryptocurrencies, CBDCs, or other digital assets, are innovating at a rapid pace.

As technology develops, the world is becoming smaller and our markets more integrated, meaning that our need for effective regulatory collaboration is only deepening. If we do not work together, we both risk our financial centers having analog rules for the digital age.

In certain respects, this review of the rules has already begun. The UK government is currently undertaking a package of measures through the financial services and markets bill and the Edinburgh Reforms to shape our post Brexit regulatory regime. The City Corporation has been heavily engaged with the government to ensure that the new rules will make the UK's regime open, competitive, and proportionate. And I am in active dialogue with our city minister, Andrew Griffith MP, who is responsible for financial services.

Our expert policy officers have provided parliamentary testimony on areas including cryptocurrencies, and we regularly convene high-level engagement with businesses, legislators, and regulators on critical topics to shape effective policy. For example, our Net Zero Delivery Summit is a milestone in the sustainable finance calendar, and we're immensely grateful that Special Presidential Envoy for Climate Secretary John Kerry could attend last year.

So as we begin to shape the future of financial markets, let us choose collaboration over confrontation. Working together, we can ensure that the Anglo-American transatlantic corridor remains a significant driver of prosperity and growth for both our countries. And in doing so, we will put ourselves in a better position to tackle global issues that are integral to both our countries -- achieving net zero, building sustainable growth, and securing open economic partnerships.

It is in this spirit of partnership that the City Corporation has well-developed plans for a United States office, which we hope to launch before the end of the year. It is our sincere hope that this move will only strengthen our ties with our single largest trading partner. Because given the global challenges before us, now, more than ever, our economies and our countries need to stand together.

Thank you.

CHAIR CRIGHTON: Thank you, Chris.

And now we'll turn to Future of Finance Subcommittee issues. This section will have two panels. First, I'm pleased to introduce speakers who will present on developing a regulatory framework for digital assets.

First, former CFTC Chairman Tim Massad, now from the Harvard Kennedy School, will offer his insight on critical policy considerations. We'll hear from

Valerie Szczepanik, Director of the SEC's Strategic Hub for Innovation and Financial Technology. We'll also hear from Eun Young Choi, Director of the National Cryptocurrency Enforcement Team at Department of Justice.

Following Eun Young, Mark Hays, senior policy analyst for Americans for Financial Reform/Demand Progress, will present. And finally, we'll hear from one of our MRAC members, Alessandro Cocco, from the Federal Reserve Bank of Chicago.

Tim, please get us started.

MR. MASSAD: Commissioner Johnson, Chair Crighton, and staff, thank you very much for the opportunity to speak to you today.

It has been almost a decade since I first testified before Congress about the need to establish regulatory standards for crypto assets. Since that time, the development of appropriate regulatory standards for the crypto industry has been hampered by interminable debates over whether particular digital assets are securities or commodities or something else.

While the collapse of FTX and other crypto firms has increased calls for better regulation, there is not yet a consensus on the path forward. The simple truth is the industry does not today comply with investor protection standards comparable to other financial markets, and hundreds of thousands of people have suffered losses.

Crypto industry participants have exploited jurisdictional gaps and argued that most digital assets should not be treated as securities, but instead as commodities where the spot market has no federal regulator. The CFTC and the SEC have brought important enforcement actions, but these efforts have not been sufficient to raise overall standards to a basic level of investor protection. Various legislative proposals have been made, but there are very divergent views in Congress on what to do.

There is, however, a solution that the CFTC and the SEC could implement today that does not require new legislative authority. It requires only cooperation between the agencies, creativity, and a willingness to implement some reasonable baseline standards now, even if these do not provide a comprehensive solution.

It starts with recognizing two critical facts. The first is that the investor protection measures we want are largely the same, whether a crypto asset falls in the securities bucket, the commodities bucket, or a yet-to-be-defined third bucket. And the second is that, for all the novelty of blockchain technology, most crypto trading isn't recorded on chain but rather on traditional ledgers kept by centralized intermediaries. These entities claim the products they trade don't make them subject to registration with either the SEC or the CFTC, which means that investor protection rests on state laws written for the telegraph era that are woefully inadequate.

The solution is for the CFTC and the SEC to create some common minimal standards, starting first with requirements for centralized trading platforms. This could be done directly by the agencies, as former SEC Chairman Jay Clayton and I have said in a recent Wall Street Journal op-ed, or through the creation of a new self-regulatory organization that would be closely supervised by both the SEC and the CFTC, as Harvard Law School Professor Howell Jackson and I have written in a

Brookings paper.

These standards could include the following. Requirements for the custody and safeguarding of customer assets, including prohibitions on comingling or lending of customer assets. Prohibitions on the operation of conflicting businesses, such as proprietary trading. Prohibitions on having economic interests in crypto tokens listed or traded on the platform. Prohibitions against fraud, manipulation, and abusive practices, including in particular wash trading. And this would also include requirements to develop or contract out for adequate surveillance and detection systems.

Execution and settlement of transactions in a competitive, open, efficient, and timely manner. Pre- and post trade transparency requirements, recordkeeping, and periodic public disclosures. Governance and fitness of directors, and basic risk management, operational resilience, and cybersecurity standards.

As former Chair Clayton and I have written, one could also require platforms to only accept those stablecoins that meet certain requirements to help ensure stablecoins are, in fact, stable. Adopting some basic standards through this approach would dramatically improve investor protection and might take some of the speculative wind out of the sector's sails.

Imagine if we simply prohibited wash trading, which has been estimated to account for 50 percent or more of the trading on many platforms. And that would also be beneficial in detecting illicit activity.

Former Chair Clayton and I have proposed that the CFTC and SEC could tell trading venues adopt these standards for everything you trade if you haven't already registered with the SEC or the CFTC directly, and this would establish an interim period where an intermediary would not be shut down for failure to register as long as it complies with those standards.

Similarly, as Professor Jackson and I have written, while the CFTC and the SEC may not have the formal power to require crypto firms to join an SRO, we believe the agencies could create powerful incentives to encourage membership and compliance with SRO rules. The responsible members of the crypto industry would have every reason to join such a well-regulated SRO once created, and it would also involve the industry in paying for the development of such standards. This approach would not involve changing our traditional standards for the definition of securities and derivatives, nor would it undermine the authority of either the SEC or the CFTC.

Now I have suggested the focus be on centralized trading venues. This does not mean decentralized platforms should be given a free pass. I am simply suggesting we take it one step at a time, and it is a step that is long overdue.

Thank you.

MS. SZCZEPANIK: Thank you to the CFTC, Commissioners, and the MRAC for inviting me to speak.

I am Val Szczepanik. I'm the Director of the SEC's Strategic Hub for Innovation and Financial Technology. I speak in that capacity and not necessarily on behalf of the Commission or any commissioner.

I've been working on distributed ledger technology and crypto assets at the SEC since 2012 in my various roles at the SEC, both in the Enforcement Division and in the Division of Corporation Finance and, most recently, at my post as the Director of SEC's FinHub.

FinHub was formulated partly to engage with innovators and entrepreneurs and developers in this space and to set up an active engagement so that we can talk about emerging areas and how our laws apply and how we interpret the federal securities laws and, in a sense, the broader frameworks and public policy frameworks that apply to activities in the financial industry. We've had broad and deep engagement over the years in this technology and its various opportunities and applications.

Our efforts are to balance innovation with the federal securities laws mandates, which are to protect investors, ensure market integrity, and promote capital formation. And I think innovation cannot happen at the expense of investor protection, nor can it happen at the expense of market integrity. Only when it happens and consistently with regulatory frameworks will we achieve the benefits in a long run.

And so the approach that we've taken at the SEC has been consistent through the years. As our chair has said, many, if not most, of these crypto assets that we're seeing are offered and sold as securities. I agree with my esteemed colleague Tim that wouldn't it be nice if we had protections against fraud and then ensure market integrity. We do have those protections. They're called the Federal securities laws.

And so we have a framework that does apply. The '33 Act, the '34 Act, and the '40 Acts provide important protections governing full and fair disclosure around the offer and sale of securities, governing market integrity, preventing against market abuses, insider trading, unfair practices, and guaranteeing fair, efficient markets.

And so we've been encouraging folks to come in. There has been a lot of noncompliance in this space, and I think, unfortunately, what we've seen over the past year has been the result of folks acting in noncompliance and has resulted in quite a lot of investor harm.

So, at the SEC, we don't -- we take a technology neutral approach. We are encouraging folks to come in and to register appropriately their offerings and to register as intermediaries as appropriate. We've been focusing on offerings; trading, lending, and borrowing platforms; stablecoins; DeFi. I think our chair has spoken recently about looking at vertical integration of the products and services offered through either a single entity or group of affiliated entities and thinking about whether or not these types of services and products should be broken out, separately registered and regulated. And so we've been working very hard on these issues.

I would say across the Commission, digital assets, crypto assets have been integral parts of our work. We've been -- for example, in the Division of Corporation Finance, our staff has been reviewing filings that come in. We've had companies register offerings of crypto asset securities. We've had companies have offered these things pursuant to an exemption and had offering circulars qualified.

So these things are happening, and there is a lot of talk that it is impossible to do this or that, but

I'm telling you that we have been applying the Federal securities laws in this space effectively. We have divisions who are doing rulemakings and putting out rulemakings, asking for input around questions concerning crypto assets. And so those rulemakings are out there, and we are taking in public input and considering that in the course of our work.

We do have a Division of Enforcement that has been enforcing the Federal securities laws in this space. We've brought a number of pretty high-profile cases lately and, I would say, showing the kinds of harm that's happened in this market.

We have several cases involving lending and borrowing programs that brought in a lot of retail investors without adequate disclosure, as alleged in those complaints. We've got a couple pretty big Ponzi schemes that have been alleged out there. And so our strategy really is bring investor protection and market integrity to this space, plain and simple, and we're working across the Commission to do that.

How else are we doing that? We're really cooperating and working collaboratively with our domestic partners, including the CFTC. For years, the CFTC and SEC staff have worked collaboratively and hand-in-hand to coordinate in this area. We also work with the Department of Justice, FinCen, and our other Federal financial regulators, including in the banking sector.

And we're also very involved internationally. So there is a lot of work going on through the Financial Stability Board looking at high-level recommendations that would apply to crypto assets and stablecoins. IOSCO has set up a FinTech task force, and we're very involved in that. There is, right now, two workstreams going on. One involving DeFi that the SEC staff is chairing, and another involving more centralized activity that the UK FCA is chairing. And so we work very closely with our partners across the pond and in the UK on that work.

And so I just would encourage folks who are members of the public to look at what the agencies are doing, to engage with us through our financial innovation hubs, and to also provide public input when input is asked for by the agencies. And you can take part in a lot of the work that is going on.

Thank you.

MS. CHOI: Good morning. Some tech problems, which is a little bit disturbing.

But good morning, and thank you, Commissioner Johnson and Chair Crighton and the Market Risk Advisory Committee, for inviting me to speak here today.

My name is Eun Young Choi. I'm the Director of the National Cryptocurrency Enforcement Team from the Department of Justice, and I'd like to just give a brief overview of the work that we're doing with the NCET at the Department of Justice with regard to regulatory policy and a legal framework for digital assets going forward.

To give a little bit of background, the primary ambit of the Department of Justice and its role in the digital assets space is to ensure that we are well positioned to combat the criminal misuse of digital assets. That spreads beyond market integrity, and I think it's probably important to note that our work at the Department in this area started with fighting money laundering against digital asset platforms even before the advent of cryptocurrency, which I think is an important framework to work with.

Our perspective is as follows. We started looking at criminal misuse of cryptocurrency in particular with the growth of darknet markets, starting with Silk Road. And since that time, we've seen an increase not only from our perspective in the number of darknet markets that have grown since the wake of Silk Road, including not only the number, but also the volume of transactions on those platforms. But also the ways in which digital assets have been misused by criminal actors across a variety of different types of work.

So it's not just narcotics and contraband transactions as you would see in these darknet market contexts, but also thefts and frauds of all kinds, cyber crime, including ransomware, national security threats, including, for instance, efforts by the North Koreans to avoid sanctions enforcement. And from that perspective, we're looking to see really whether or not our criminal authorities are adequately dealing with the challenges posed by digital assets.

And so our work at the NCET started in January

2022. And the purpose of the NCET and the reason why the Criminal Division started the NCET was because there was a recognition by the Department that the use of digital assets has become very cross-cutting and multidisciplinary in our work, and we were seeing it in all different types of criminal investigations.

Thus, we set up a group of subject matter experts, which I lead, that support the investigations and conduction investigations into the criminal misuse of digital assets, with a particular emphasis on centralized platforms that are used to commit a variety of illicit finance risks, as well as to set priorities and policy for the Department, bringing all of the stakeholders to the table.

Over the last year, most of our work has been directed towards our involvement in the development of and the work under the executive order that was signed by President Biden in March of 2022 entitled Ensuring Responsible Development of Digital Assets to Address Risks and Harness the Potential Benefits for Digital Assets and Related Technologies. That particular executive order identified six key priorities for work across the interagency.

Those include consumer investor protection, promoting financial stability, countering illicit finance, U.S. leadership in the global financial system and economic competitiveness, financial inclusion, and responsible innovation. And from that work, the Department of Justice in particular has written two reports. One on how to strengthen international law enforcement cooperation for detecting, investigating, and prosecuting criminal activity related to general assets, released in June. And then the role of law enforcement in detecting, investigating, and prosecuting criminal activity related to digital assets, which came out in September.

The culmination of those efforts led to the administration's issuance in January of 2023 of the Roadmap to Mitigate Cryptocurrency Risks. And I think it's important to note that all of this work was done in the wake of a remarkable increase in the market path of the digital asset markets reaching its peak of $3 trillion in November of 2021 and then the ensuing "crypto winter," where prices and trading volume fell dramatically. Several high-profile companies collapsed, and there was an increase in what we see as illicit finance risks and the other criminal risks that I spoke about earlier.

So in that wake, the Department of Justice set forth specific challenges that we see as with regard to digital assets technology as it pertains to our criminal investigations and our mandate. I think it's important to note that many criminal assets and products in the DeFi and digital assets space function akin to tradition analogs, and so our criminal authorities should be equally applicable to those new products in order for us to be able to keep the American public safe from the risks posed by digital assets.

As a result, we have set forth specific legislative proposals for the administration's consideration. Among those are amendments to the Bank Secrecy Act, anti-tipoff statutes that are used in investigations involving financial institutions to be expressly applicable to the area of digital assets, laws against the unlicensed money transmitting businesses and their applicability to digital asset platforms, and amendments to several Federal statutes that deal with jurisdiction and venue issues in order to deal with the cross-cutting and international nature of these types of digital asset crimes.

So, with that, I would just like to note that every day, the Department of Justice works to keep the American public safe, including from the risks that are posed from digital assets. It's important to recognize that with innovation comes the responsibility to ensure that there are safeguards that will make sure that the technology cannot be exploited by bad actors, and we look forward to working with our partners across agencies on those challenges moving forward.

MR. HAYS: Good morning. Thank you for the opportunity to speak with members of the advisory committee, the Commission staff, and of course leadership, as well as my fellow panelists.

My name is Mark Hays. I'm a senior policy analyst with Americans for Financial Reform and Demand Progress. And there are many topics related to digital assets that would make sense for the Commission's review, given the complexity, uncertainty, and volatility of this space. And with limited time, I want to spend the bulk of my remarks on really two areas of focus and further study.

I should say at the outset that our organizations, who are focused on a wide range of financial reforms to protect consumers, investors, and financial markets and promote racial and economic justice and equity throughout our financial system, take a skeptical view of the use case of digital assets in achieving some of those aims. We're concerned about the widespread sort of illicit and unethical activity we find in crypto marketplaces today. We're concerned about the nature of the business models, which aspire to provide more financial inclusion, but often end up mimicking predatory financial activities we've seen in traditional markets, and we have concerns about the structural limitations of the technology itself.

Our perspective really is informed by wanting to use the same consistent, robust regulatory standards that apply across financial markets and ideally those that prioritize protecting consumers, particularly lowincome consumers and people of color, as opposed to creating special carve-outs for industries, whether it's digital assets or others.

So, with that in mind, I think we are encouraging policymakers to use the existing tools they have robustly and effectively and consistently, and then any new proposals that are put out are not geared to make exceptions but are rather geared to promote consistency and those priorities.

So there are two topics that we're interested in for the purposes of this meeting today. The first is looking into how the CFTC could gain better visibility into the integrity and management of businesses that seek to acquire ownership stakes in registered entities with the Commission.

And I know Commissioner Johnson raised this in a speech last January, referencing FTX acquisition of LedgerX. That acquisition offers a lot of interesting lessons on both positives and negatives of what that regime was able to do, but the acquisition itself raises questions about how that pattern of acquisition fosters risks in the digital asset space.

That acquisition isn't unique. While the models differ, we've seen FTX allegedly pursuing other acquisitions to find back doors and regulatory arbitrage gaps. We're hearing news reports about other platforms like Binance using similar strategies. And so it really raises questions about what those acquisitions are intended to do.

Of course, many of those acquisitions are benign and conventional. That's certainly clear. But given that, for example, many crypto firms operate offshore, and there is limited sightlines for the CFTC and other agencies into those acquiring bodies, it's important and we agree that the CFTC should use all their existing tools and authority to carry out and, if needed, deepen the due diligence they do on such acquisitions.

And we believe the CFTC should be exploring what additional authority or resources may be needed to enhance such efforts. And we believe the MRAC could assist with this in a few ways.

First, the committee could lead a review of other recent acquisitions of CFTC registrants exposed to digital assets to identify any anomalies or find best practices of due diligence done well. Second, the MRAC could identify procedures employed at other agencies, sister agencies, that might gain some insight into other best practices that could be migrated over to this space.

I note that with broker-dealers, the SEC, FINRA, and SROs provide a fairly robust due diligence practice. It's not perfect, but there are lessons to be learned there. That could also be a stepping stone to better coordination between agencies, given that many companies that are likely to acquire Commission-registered entities may be primarily regulated in another space.

Our second recommendation is to explore the topic of cybersecurity threats for blockchain products in general and for crypto derivative markets more specifically. Currently, crypto derivatives trading don't typically occur directly on the blockchain, but on more conventional trading platforms. But the underlying assets for these trades do exist on the blockchain, which means the risks there can be translated into operational and market risks.

Now the rhetoric around blockchains often asserts that at its core that the mutability of the chain and its protocols provides potentially a higher level of security for financial platforms than currently exists. We know the reality is often far different. Like any software program or computer network, these platforms are just as vulnerable to cybersecurity risks.

There are a long list, which I won't go into, but the code can contain bugs that offer hackers opportunities, or it can be engineered by inside players to perform exploits. Flaws in codes can execute transactions that end up being harmful to participants, but with limited ability to stop them. New layers of code that are added to deal with slow transaction speeds or interoperability can become some of the most vulnerable points of attack.

And these are just the operational security challenges. We're not talking about structural vulnerabilities dealing with ISPs or data storage, as well as some of the other frauds, affinity scams, and ransomware issues we've discussed today that have migrated to the blockchain and thrived there.

So, with that, we would recommend that the MRAC review the linkages between cybersecurity risks found on blockchain platforms tied to existing crypto derivatives, both that operational risk as well as that underlying structural risk. And the MRAC could identify opportunities that can ensure integrity of movement and pricing of assets on the blockchain and help better protect customer funds, as well as identify better standards of custody that could guard against cybersecurity risks.

So, ultimately, we think that review could recommend -- could generate recommendations on how to strengthen the CFTC's overall cybersecurity requirements for the platforms that house and generate the assets that underlie those derivative markets.

Thank you for your time today. I'd be happy to answer any follow-up information or questions on those topics for discussion.

MR. COCCO: Commissioner Johnson, Chair Crighton, Chief Counsel Fekrat, Special Counsel Dahlman, many thanks for inviting me to present today. It's great to be here with you, Commissioner Goldsmith Romero and Commissioner Pham, as well as the many talented policymakers, market participants, policy advocates, and academics on today's panel.

The topic I'd like to address today is liquidity risks to backing organizations resulting from crypto asset market vulnerabilities. Liquidity is central to the stability of the financial system. Much of the work of this committee focuses on risks affecting clearing and financial market infrastructure, and digital assets are a new addition and present new challenges and opportunities in the context of financial market infrastructure.

Before I go any further, let me say please that the views I express today are my own and not those of the Federal Reserve.

To a great extent, clearing transforms counterparty risks into liquidity risks, and for that reason, it is appropriate to monitor liquidity carefully in the context of cleared products and to work on policies that support liquidity in these markets. As we learned from several events in the past 12 months, liquidity is also a key factor in the context of crypto assets.

As crypto asset companies have come under strain over the past year, regulators have looked carefully at how these companies interact with banks and what liquidity strains could potentially be passed from the crypto asset sector to banks. Today, I'd like to talk about the Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto Asset Market Vulnerabilities. The statement was issued just a few days ago on February 23rd by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency.

The topic of the statement is the liquidity risks to banking organizations presented by participants in the crypto asset markets. The statement also addresses some practices to manage these liquidity risks.

So let's go through what the statement says. Banking organizations are neither prohibited nor discouraged from providing banking services to any customer so long as the provision of these services is permitted by law or regulation. The statement does not create new risk management principles, but rather reminds banking organizations to apply existing principles.

The statement then goes on to highlight the liquidity risks posed by deposits with a banking organization by a crypto asset-related entity for the benefit of that entity's customers, as well as liquidity risks for deposits that constitute stablecoin-related reserves. In both of these cases, the banking organizations may be susceptible to large inflows and outflows as a result of periods of stress, market volatility, changes in consumer sentiment, and vulnerabilities that may or may not be specific to crypto assets.

In the case of deposits placed by a crypto asset-related entity for the benefit of that entity's customers, these large inflows and outflows will be driven by the behavior of that entity's own customers and not just by the entity itself, even though that entity and not its customers are the client of the banking organization. In the case of stablecoins, these inflows and outflows may be linked to unanticipated stablecoin redemptions. These liquidity risks may be heightened further if the deposit funding base of the banking organization is concentrated in crypto asset-related entities that are correlated.

The statement then goes on to remind banking organizations of some of the risk management practices that can help address the liquidity risks from crypto asset-related entities. These risk management practices include developing an understanding of the factors affecting deposits from crypto asset-related entities and identifying whether these deposits are susceptible to unpredictable volatility.

Evaluate potential interconnectedness and sector concentration. Take into account the liquidity risks and funding volatility that are specific to deposits related to crypto assets in the context of broader contingency funding planning and liquidity stress testing. And then, finally, conduct robust due diligence and ongoing monitoring of crypto asset-related entities who open and maintain deposit accounts, in particular with respect to circumstances that could result in rapid outflows of these deposits.

The statement then reminds banking organizations to comply with all applicable laws and regulation such as compliance with call reports for insured deposit institutions. So these principles are designed to assist banking organizations in managing liquidity risk in the event they provide banking services to this growing crypto asset infrastructure and are designed to contain potential spillover risks between the crypto infrastructure and traditional finance.

This concludes my remarks.

CHAIR CRIGHTON: Great. Thank you very much for all of those remarks. Very informative.

We'll now turn to the second panel of Section 2 and continue the future of finance discussion. We have five distinguished speakers for this panel. Brad Levy, Chief Executive Officer for Symphony, will open the panel. Then we'll turn to Hayden Adams, Founder and Chief Executive Officer of Uniswap Labs. Next, Candace Kelly, Chief Legal Officer for Stellar Development Foundation will present. Following Candace's presentation, we'll hear insights from Linda Jeng from the Crypto Council for Innovation. And finally, Caroline Malcolm, Global Head of Public Policy for Chainalysis, Inc., will speak.

Following the presentations, we'll open the floor to MRAC members.

Brad, I'll turn it to you.

MR. LEVY: Thank you very much.

I have some slides. Thank you very much.

So moving beyond common use cases, the title of our section here -- and it's not common today, but I think the view of our panel will be it will be more common in the future -- I'll be focusing on interoperability more generally and identity. I have my crypto-cousins in a more distributed world with me, and I'm looking forward to hearing from them as well.

Thank you to the Commission and for Commissioner Johnson for driving and for Chair Crighton for leading here.

So if we can just page? So the future of finance -- and Chris Hayward indicated this on the regulatory front, interoperability of regulations. If we can page to the next?

I'll be speaking more to the technical interoperability and interoperability of workflow. So, more generally, interoperability is the ability of multiple systems and software applications to exchange and make use of information seamlessly. It allows for more choice at institutional and user levels, a more modular approach to technology, and a more deeply integrated approach.

There are many areas of technology that enable interoperability, such as cloud computing, platform technologies, and mobile; identity management, which I'll dwell on a bit in a moment, and the entitlements behind that; and a more embeddable technology, as well as a more extensible technology.

The benefits of this over the long term will be a better user experience in general, less institutional and more for the user and consumer, reduction of context switching, which is a major risk in the market as users move from system to system -- fat fingering, et cetera -- and will ultimately lower the switching costs of technologies over time as we build more plugin play. So with incremental innovations versus big bang, we'll likely become a more innovative, faster market and safer and more resilient in the long run.

If we can page?

So interoperability in terms of market infrastructure, one common standard I would just like to point out is an initiative developed by the FINOS Open Source Foundation, which is now part of Linux, the FDC3, where they develop open standards for the market participants, whether it's app directors and how you point to different applications that you need, the intent that you establish, the contexts, and the API structures.

So much of this in our market today is highly proprietary and embedded within systems. There is a belief that more can be open sourced, and the FDC3 standard specifically is an enabler of interoperability. It's analogous to the W3C that was the standard-setter for the world on the Internet, and another analog would be what is happening in the media space where you're able to put cable alongside of streaming apps inside of a Samsung TV on an operating system that you choose, whether it's android or Apple, et cetera.

The financial market adoption rate is still early days. The Tier 1 larger firms on the bank side are moving relatively swiftly on this, whether it's ability to launch application in their environment that can interoperate with each other or actual desktop interop.

As you move down the spectrum and maybe the budgets get a bit smaller, there is more of a blend of being able to do it yourself or relying on the vendor community more generally. And then the buy side of the asset manager community is likely to be more heavily reliant on the vendor community to drive these initiatives.

One more page.

So one area that we're focusing in on in Symphony -- and just to point out, much of our lives are pinned to an email address, an Apple ID, an Amazon account. It's maybe akin to a Social Security number. I'm not sure anybody today would rely on their Social Security number to be their identity, given it's fairly available on the planet.

So what do we do to create a better identity system that indicates you're at a firm in a role and have certain interests and have certain tasks to accomplish? So, we, at Symphony and across the industry more broadly, are working on a concept where it's an identity as a service. It's not the platform we sell necessarily, but more conceptually. How do we deal with the problem statement of disconnected identities in many different places? Authentication frictions, security breaches, a lack of industry-wide directory to deal with BAU or event-driven moments such as market crises, and increasing regulatory requirements that allow you to be known very clearly or completely anonymize where appropriate.

We all have password fatigue, and we all really struggle to figure out what data we need at any time. And just finding the right person is a challenge.

So what we believe is a more business-to-business real-time ability to indicate you're a part of an institution that would really be coming from a very core system at an institution like an HR system. That system or those datasets would need to be very unique to those individuals based on their role, and those IDs would need to be portable over time.

Ultimately, they will need to be open architecture, meaning available on many systems that choose to embrace a more open identity system, which can be enriched with your interests and your roles. And then, ultimately, leveraged in various market workflows across the front office, middle office, and back office.

So as we look to move to Web 3.0, which is hopefully a much more secure, resilient, but also encrypted where appropriate or disclosed where appropriate, we look forward to building a better identity solution for the market overall, working with many partners and industry players today while we speed up the processing times and reduce risk overall in the industry.

Thank you very much for the time today.

MR. ADAMS: Thank you, Commissioner Johnson, for inviting me to speak today. It's an honor to have the opportunity to provide some of my thoughts on blockchain use cases.

Today, I'll focus on decentralized finance, or DeFi. DeFi protocols should be seen as a tool that can help regulators and society more broadly achieve their goals of protecting consumers and improving markets and not at all at odds with those goals. I invented a DeFi protocol called Uniswap that allows the exchange of any two assets on Ethereum-based blockchains. The protocol is open source, publicly available code that operates without any involvement from custodians or exchanges and no involvement from me or my company, Uniswap Labs.

It has supported more than 1.4 trillion in volume since November 2018, mostly in assets that the CFTC has determined to be commodities, such as bitcoin, Ethereum, and stablecoins. It has run 24/7 without any downtime and has never suffered a hack.

DeFi protocols are a rules-based, autonomous software with transparent code that can be an alternative to intermediaries in some transactions. Bitcoins could be considered the first DeFi protocol because it allows custody and payments without intermediaries. Today, DeFi protocols include some offering peer-to-peer lending or asset exchange without intermediaries.

Uniswap was designed to utilize core benefits with blockchains, accessibility, transparency, and market activity without the reliance on intermediaries that can cause fraud, error, or other risks. I'll briefly address each of these benefits.

On accessibility, the appeal of a more accessible and fair financial system is at the heart of the adoption of digital assets by 15 to 20 percent of Americans. Failure among banks during the 2008 crisis made many Americans believe that there was one set of rules for the powerful and another for the rest of us.

DeFi protocols do not make allowances for the politically connected or the too big to fail. Indeed, users are increasingly turning to them in the digital asset space. Post 2022 among digital asset investors, on-chain data shows that there is a shift away from centralized exchanges to self-custody and DeFi.

On transparency, decentralized finance protocols are transparent and when properly designed should not be able to be unilaterally altered by any one person or company to the detriment of users. Transparent natively digital records could help accomplish the goal of post financial crisis regulations to make markets more open, transparent, and competitive through software.

For example, enacting the CFTC's post financial crisis rules for pre- and post trade transparency and open access, which aims to increase competition and financial stability might be done by any participant on a DeFi protocol in minutes.

Finally, on operating without intermediaries. Intermediaries often require considerable regulation because they can make serious mistakes. They can cheat people, and they can pose systemic risks. The DeFi protocols allow users to maintain custody of their own assets.

To use Uniswap as an example, users maintain custody of their own assets, and trades only happen according to predetermined rules that cannot be amended. For this reason, DeFi does not have the same risks as centralized exchanges, where the exchange is hacked or the owner of the exchange can simply steal a user's assets and gamble them away.

This is not to say that DeFi does not have risks of its own, particularly hacks and scams. DeFi hacks can occur where there are bugs in the code or if a form of centralized control is interjected in the protocol, such as with some cross blockchain bridging protocols. Hack risk can be reduced through coding best practices, robust independent cybersecurity audits, better self-custody technology, and real, true decentralization.

Similarly, there are ways to greatly reduce the risk of scams. Much of this risk is the result of the stage of development of the technology and the need to build safeguards in any new technology and is not specific to the technology itself. Educational efforts, better disclosures, and token screening products as well as regulation can help, like standardized digital asset disclosures under EU's MiCA.

We and many others are eager to explore with policymakers how to make decentralized digital asset technology more secure. The CFTC has an important role to play in providing rules of the road to protect users of both centralized digital asset platforms and DeFis and to harness new technologies to achieve the same or better policy outcomes.

Thank you.

MS. KELLY: Commissioner Johnson and Chair Crighton, thank you so much for inviting us to this conversation. It's really just so fabulous to have this public-private discourse.

And in the context of risk, which we're hearing a lot about today, I would like to focus on the question that we at the Stellar Development Foundation, given our mission of creating equitable access to the global financial system, we focus on the question of what is blockchain good for? All day, every day. And it's a question that has come up more and more in public discourse today.

And so our answer is with respect to the exchange of value, speed, security, cost, and accessibility. And I want to talk to you today about a few uses that are happening today and some that are being built on the Stellar network that are leveraging the technology to take advantage of those benefits of the technology.

First, I'll just say that the Stellar network is an open and public network, and it is optimized for cross-border payments and for asset issuance. So when I say that, the most prevalent assets that we see on the network are fiat-backed stablecoins and tokenized assets, which, of course, require additional controls by the asset issuer, which are available through this technology.

So I'd like to talk about a couple of examples that are happening today. The first is MoneyGram. So MoneyGram has, as you all probably know, over 300,000 agents in locations across 180 countries. They have a very heavily cash-dependent user base, and when they realized that there are all of these benefits from blockchain technology, they created MoneyGram Access, which they are rolling out across all of those agents across the globe.

And what that means is that a user can walk into a MoneyGram agent. They can hand them cash in their local currency. They can have that cash sent to their digital wallet in the form of USDC, Circles, fiat-backed stablecoin. And then that person is -- has access to the digital economy.

And one of the things, given our mission, that we are so thrilled about is that someone can use a self-posted wallet with that USDC and send those tokens back home in a remittance where -- I'm from California. So I think of the migrant population sending money home to Mexico.

So if that person's mom receives those USDC tokens, one, she can hold them because it's a very stable currency to hold something that's backed by the U.S. dollar. And if and when she needs to use it in the local economy, she walks into her local MoneyGram agent and cashes that out into her local currency in pesos. So, of course, it can go back the other way as well, from USDC back into fiat.

So that is I think one of the important things that we have focused on in pursuing our mission is that blockchain is a tool that is not meant necessarily to replace the global financial system, but to enhance it and interoperate with it. And I think that MoneyGram access example is a really great one to highlight that.

So when the war on Ukraine broke out, we were contacted by the U.N. High Commissioner for Refugees, who was aware of the MoneyGram Access service and said, you know what, if we can scale that, that will help solve the problem of getting cash aid to humanitarian recipients in Ukraine and in the surrounding countries. And so, MoneyGram, Circle, the U.N., the International Rescue Committee also helped work on this project us, spent a long time last year trying to take the MoneyGram Access use case and enhance it with a bulk disbursement tool.

And by the end of the year, we were able to pilot that with the UNHCR and the IRC to get aid in the same way that I just described. So donor funds transferred into USDC get into the hands of folks in Ukraine. And if you think about the situation in Ukraine and the fact that someone can be sitting in their home or, in many cases, in a bunker and receive these digital assets in their wallet, and then they have the power to go either to an agent. A lot of the Ukrainians don't have the challenge of being underbanked or unbanked, and so MoneyGram can help them just do an ACH wire transfer in local hryvnia into their bank accounts. It's an incredibly powerful tool.

Of course, there are some who may end up leaving Ukraine and ending up in a different country. So the power of having a U.S.-backed -- a U.S. dollar-backed token in their wallet and go into a MoneyGram agent in Poland, Slovenia, wherever they end up, and be able to cash out in local currency rather than having to try and get a bank account and see whether or not they're going to take hryvnia and what the value of that is at any given time is another powerful solution that this Stellar aid assist is providing for in the humanitarian aid.

So what is blockchain good for? Humanitarian is one answer to that. And then I'm going to run through some of the other ones more quickly in the interest of time. But on the next slide, another answer to that is international payroll.

So we are living in a world where there are more and more international workers. There are more and more remote workers who are working in different countries and being able -- for companies to be able to send payroll efficiently, effectively, and without increased cost in the currency, whether it's a cryptocurrency, a stablecoin, or fiat currency, to workers is also a powerful tool.

So I'm going to -- you have access to the slides. I'm going to skip to the very last one because I think it's important to talk also about regulated assets.

So Franklin Templeton I think is the best example of issuing regulated assets on a blockchain network. So they are the first U.S. registered mutual fund that issues tokens -- they are called Benji tokens -- that track the transactions and the ownership of those tokens.

And of course, the technology has these additional features that allow them to do that and be able to comply with their compliance obligations. They can approve users before they can hold or transact those tokens. They can freeze accounts. They can have clawback of assets. This is all on an open public network if the asset that the issuer has these extra controls on, that is the power of this technology.

So, with that, I want to just say that I hope that having a couple of insights into -- and there's a few more in the slides -- real-world use cases is helpful in this public-private dialogue. Because we hope that in working with regulators and policymakers that we can craft enforcement and regulatory frameworks that allow the innovations to flourish, and so we can continue to see this innovating network thrive and reach users and solve the cost, speed, security, and financial access challenges that we see in today's traditional markets.

Thank you.

MS. JENG: Hi, I'm Linda Jeng. I'm with the Crypto Council for Innovation, and thank you, Commissioner Johnson, for inviting me to speak today.

You asked me to speak on any topic of my choice, and I took you up to discuss decentralized identity. We are moving towards a future where we're going to be not just an economy of manufacturing, but an economy of digital data. And so if we're going to have a digital economy that's going to be built essentially on technology stocks, the most important stock will be our digital identity.

So, next slide, please.

I personally detest the term "decentralized identity." It makes me feel like identities all over the place and is actually the opposite of what a decentralized identity solution is about. It's actually about empowering the individual to custody and manage one's own digital assets.

Next slide, please.

So I'm going to just jump very quickly through these slides and happy to discuss more with any of you later. But decentralized identity, which I like to call self-custodied identity, brings up a number of very important themes for our digital economy.

Next slide, please. Next slide.

And what is really important is as we are transacting in a digital economy, one of the most difficult things to do is to verify your identity remotely, and this is what a self-custodied identity should help you to do as we participate in online thinking or even DeFi.

Next slide, please.

So the Internet, as we all know, was developed over the past five decades, beginning in the '70s. It did not include an identity layer, and this is why we have essentially data proliferation of multiple accounts, usernames, passwords, with companies all around the world.

Last night, I actually tried to sit down and count the number of account names and passwords I have. I stopped at 75. I still have many more, and I actually don't remember most of my passwords. And so I'm pretty sure I'm not the only one, and this is a serious problem not just for as a user experience, but also for cyber crimes, which we were just discussing earlier today.

As in order to open up accounts with companies online, you have to provide your personal data, and they store your personal data and, in turn, provide you with an account name and password. This creates honeypots across the entire online ecosystem.

Next slide, please. Next slide.

Sorry, I have to go through this really quickly. Next slide. Yep.

And so what happens is you essentially have your personal data federated across multiple banks, broker-dealers, even D.C. Public School System -- like that's me -- and IRS, et cetera.

Next slide.

So we see this issue of our data not only proliferated across the economy, but also the fragmentation of our data and our inability to control our own data.

Next slide. And next slide.

Ultimately, this leads to a terrible user experience, and we actually have one of the worst digital identity report card grades in the globe.

Next slide.

So a solution that has been -- that's being currently explored by a number of technologists have been the idea of self-managed identity, and this alternative --

Next slide.

-- would mean I could go to my bank, which has KYC'd me. So I'm a customer of Bank of America, but I would go to Bank of America -- I've been with them for many years, and they would issue me a KYC verified credential.

I collect that in my digital wallet. I also collect a mobile driver's license from the D.C. DMV. As you know, a number of DMVs across the country -- currently, California and, actually, Maryland next door -- have been working on MDLs. You will collect that in your wallet.

And then, essentially, you'll collect credentials from anyone you have a relationship with, whether it's perhaps Amazon or your social media accounts or your employer, et cetera. These all represent your dynamic identity.

And then when you decide you want to get a mortgage, you can go to -- and I'm going to say here that it would be Citibank. I would go to Citibank and say, hey, I would like to get -- apply for a mortgage, and I'm going to choose which one of my verifiable credentials to share with you to meet your needs to confirm that I am who I am.

So I would share with them my KYC credential from Bank of America along with my credentials from the IRS that I have been filing, my tax forms, and my employer's credential saying that I am employed, et cetera. So it's really about self-empowerment, your ability to control your data.

Next slide.

So all this technology has been open source. You can find them on GitHub, and the technology is actually here today. And the issue is now really developing a regulatory framework to support it.

Next slide, please.

So I had pretty much -- I think I'm just going to stop here because I did put together a demo, but it -- actually, I'll just take you to the next slide.

So this is actually how it'll work. We can't do it because the way -- it only works in Google Docs, but the left side would actually be your phone, and the right side would be your laptop. So, essentially, go to your Bank of America website and just click on, hey, I want a KYC credential. And then it pops up with a QR code, which you would use your phone to scan, and then that's how you log your KYC credential onto your digital wallet.

So, thank you.

MS. MALCOLM: Thank you very much, Commissioner Johnson, for this opportunity and to your staff for facilitating this excellent discussion and overall furthering the exchange of insights between the public and private sector, which is really critical for this space, given how quickly it moves and the degree of technological innovation that we continue to see.

I'm Caroline Malcolm. I'm the Global Public -- Head of Public Policy at Chainalysis, the leading blockchain intelligence company. I've been working on blockchain and the digital asset sector for over 5 years. I set up and led the OECD's Global Blockchain Policy Centre from 2018 through to 2021, and since then working with Chainalysis, really sitting at the heart of data through which policymakers, regulators, and supervisors, as well as the industry, use to understand the sector. So I'd like to bring a global, but also a data-sound perspective to this conversation.

When I think about the CFTC's vision to be the global standard for sound regulation in the context of digital asset markets, I think there's a risk that a lot of time is spent right now, particularly in the U.S., focusing on this question of mandate. And I know a number of you have already discussed that earlier today, and I, of course, encourage the further exploration of solutions to that issue, which continue to take place in Congress.

However, I think that for the purposes of this discussion, that can sometimes be a red herring, and it risks deflecting from the most important question of what can be done now and the things that the most important people in this room can actually control.

So I'd like to be a little bit more pragmatic and specifically to emphasize that there is a significant untapped opportunity which currently exists to draw on and build on the Commission's capabilities not just in relation to surveillance, but for example, through expanding economic research to ensure that you, as a critical regulator to this space, both have a robust understanding of the sector and are well placed for the future in a ministry that does move so quickly. That includes both an understanding at the macro level of overall market structure through the specific considerations of market conduct, which have been mentioned as a concern by many already today.

In practice, that means really getting to grips with the data, with the add of the possible in blockchain intelligence, and that's really essential to bring an innovative approach to developing rules and undertaking surveillance that facilitate orderly, efficient, resilient, and robust markets.

For example, that might be data regarding the number of market participants and actors, the degree of concentration and the degree of interconnectedness between those different players and, of course, between traditional -- between this market and other markets.

First, really understanding what information you might already have to hand to really understand, for example, what is available to you through on-chain data and thinking about how to combine that with any future reporting requirements. So that information, which is on hand, which is not only available in real time but, importantly, reverses some of the information asymmetries that you may be used to when overseeing traditional markets.

When I think about the work that we do at Chainalysis, working with other countries, with other government agencies, whether it be policymakers, regulators, all those doing the day-to-day supervision of market actors, really thinking about how they bring a data-first approach to comprehend those issues. So whether that be to really understand how issues like market conduct, wash trading, pump-and-dump schemes, trade volume inflation, and using the information that is already at hand to start to build a much deeper understanding of what is actually happening in these markets, which will found not just current explorations, but also any future mandate oversight for this sector.

I also want to just close by touching on two issues highlighted by others. Firstly, in relation to this issue of illicit finance. One of the many benefits of this space is the transparency that it brings, and that means transparency in the level of illicit activity that actually takes place.

There continues to be many myths put forward about the degree to which illicit activity forms a part of this sector. And of course, while any degree of illicit activity is problematic, we also need to take it in context and understand how it fits when compared to other markets as well.

What we know from the data is that although we reached in 2022 an all-time high of just over $20 billion of illicit activity, this represents just 0.2 percent of all of the on-chain activity that took place. Now what's interesting, of course, is when we think about the digital assets sector compared to other sectors, it becomes much harder in other sectors to really get such concrete numbers, but it is important that this sector isn't, in fact, subject to penalty because it is so transparent. So we really only know in other sectors from estimates, and those estimates can vary in terms of 3 to 5 percent in terms of illicit activity that takes place.

And when we compare that to the 0.2 percent that I just mentioned, it really is a much smaller proportion. So I wanted to mention that simply to break through some of those myths, which continue to persist about the sector.

And finally just to touch on the issue highlighted by Caitlin Clarke earlier regarding national security, this continues to be an important priority in this space, an important part of an overall strategy, as been made clear from some of the speakers already. I wanted to highlight that simply because I think it can sometimes be lost when we're down in the detail of thinking about markets specifically, but there is this broader overlay of national security, which shouldn't be overlooked and of which we all have a part to play.

So I'll leave it there, but happy to take any further questions either today or in the future.

CHAIR CRIGHTON: Great. Thanks very much, Caroline and all the speakers in that panel.

I know we had indicated we would open for member discussion, but I think in the interest of time, as we are running about 30 minutes behind, we're going to hold on member discussions for now. We will allow for a short break.

I think we're going to let you take about 5 minutes, which put us back here at 12:07 p.m. to get going again. So we'll see you in 5 minutes.

Thanks very much.

(Recessed at 12:04 p.m.)

(Reconvened at 12:12 p.m.)

CHAIR CRIGHTON: All right. Thanks very much, and welcome back, everyone.

We're moving on to our third and final section of the day, which will cover matters relevant to MRAC's Climate-Related Market Risk, Market Structure, and Interest Rate Benchmark Reform Subcommittees.

To begin the discussion, it's my pleasure to introduce Scott O'Malia from ISDA, who will provide this section's opening remarks. Scott, please go ahead.

MR. O'MALIA: Thank you very much.

Good morning, Commissioner Johnson, Chair Crighton. A pleasure to be back at the CFTC and certainly before the Market Risk Advisory Committee.

Now it's almost been 3 years to the day since the World Health Organization declared COVID-19 to be a global pandemic. That moment in March of 2020 triggered the biggest shock to financial markets since the 2008 financial crisis. Within weeks, asset prices plummeted around the world, liquid assets were sold, and risk appetite disintegrated. Illiquidity in U.S. Treasury markets was of particular concern.

As we now know, liquidity shortfalls in early 2020 were not an isolated episode. And as it happens in 2022 after the Russian invasion in Ukraine drove volatility and commodity markets, again in September of 2022, the UK gilt yields rose sharply, leading the Bank of England to intervene.

When this committee was first formed, its main focus was addressing counterparty credit risk through clearing, capital rules, and margin rules. The successful implementation of those rules has made the system safer and more robust. But it's clear that the markets are now more susceptible to liquidity risk. Regulators and market participants must work together to identify and address the drivers of the recent stress events so markets can withstand future shocks.

I commend the MRAC for highlighting a number of critical issues as part of today's agenda, and I'll briefly touch on some of these topics. I would like to start with digital assets, and we've heard about the importance of -- important in a regulatory framework for the rapid development of this asset class -- for the rapidly developing asset class.

Following the collapse of the multiple crypto entities last year, it is critical that the legal foundations and fundamentals regarding bankruptcy and custody are fully considered. We need to ensure that the appropriate and clearly defined custodial and bankruptcy rules are in place and that all participants are fully aware of their rights and expected outcomes in a default scenario.

It is that we published a number of white papers on navigating a bankruptcy in digital assets, with a focus on closeout netting and collateral. Next month, we'll publish a second paper that explores the customer assets held with intermediaries and their treatment in an insolvency.

I encourage the MRAC to consider the issues as lessons to be continued to learn from as recent turmoil on the market and a counterparty risk exposure, as well as the uncertainty in bankruptcy. This is a very important issue for your consideration.

Now turning to climate risk, which will bring the topic of the next session, further work is required to build liquidity and manage counterparty risk in climate markets. We need to move quickly to create clarity around the legal framework to establish global product definitions and set high standards for voluntary carbon markets.

Without these vital ingredients, we risk fractured regional markets with insufficient liquidity. This will undermine the key objectives of driving the trillions of dollars in investment needed in infrastructure to transition to a more sustainable economy.

At ISDA, we've worked very hard to establish standard definitions and templates that can adapt to ensure climate products are consistently described and documented around the world. We'll be publishing new definitions for verified carbon credits -- we published verified definitions of carbon credits at the end of last year, and we are developing standard terms and definitions for sustainability-linked derivatives as well.

I'm also hopeful that the Integrity Council for Voluntary Carbon Markets will be successful in setting a more selective global standard for carbon credits.

The failure to establish high standards and best practices could lead to greenwashing, which will damage the confidence and stifle liquidity in this important market.

Now it was the MRAC's Climate Subcommittee that published a landmark report in 2020 regarding the management of climate risk in the U.S. financial system. The work to define appropriate risk management practices for various climate scenarios is complex and requires extensive collaboration between policymakers and the market participants.

We carried out our own survey of climate risk scenario analysis as it would apply to the trading book, and we published our findings last year. I hope this committee will continue to engage with the market on climate risk management as we work through this important topic.

Now turning to market structure, components of -- the market structure component of today's agenda, I want to reiterate is this commitment to regulatory reforms that have improved transparency in the derivatives markets. It is within this context that I expressed concerns about the changes to the CFTC's block rules that are due to take effect in December of this year.

Based on the data from 2020, we estimate that changes would raise the threshold for block trades by as much as 100 percent or possibly as high as 200 percent off the 2013 levels. Under the revised threshold made available to trade swaps that are currently traded bilaterally as blocks, will have to be executed on SEFs, subject to the RFQ of three requirement. Critically, the uncapped notional amounts of these trades will also be publicly disseminated.

The increased thresholds would have a big impact on market liquidity, exposing dealers to a winner's curse, whereby others will know how large -- what they are looking to hedge in terms of their large size. Liquidity providers will need to account for this, leading to widening of the bid offer spread, increased transaction costs, and delays in executing hedges.

A key in determining appropriate block size is the level of liquidity and risk sensitivity of a particular asset class. These measures naturally evolve over time and can change with different market conditions. We encourage the CFTC to further consult on how the revised block thresholds could impact liquidity before they come into force.

Finally, I'll touch on the U.S. Treasury market, which is the beating heart that keeps liquidity flowing in the global financial system. A number of ideas have been discussed to enhance liquidity and resilience in this market. Inefficiencies in the U.S. Treasury market could adversely affect collateral for derivatives. ISDA members would like to see an outcome that increases liquidity in this important market.

I'll highlight two particular areas that have been discussed. First, changes to the supplemental leverage ratio and the G-SIB surcharge would allow regulated banks to transact in the Treasury market in a more balance sheet efficient and cost-effective manner. Changes to these requirements are, of course, subject to prudential regulation. So I won't go into further detail here.

The second is the SEC's proposed rules that would require clearing of certain U.S. Treasury securities transactions. Part of the SEC's proposal is to carry out a survey of its membership to understand how the clearing mandate might impact that discussion. This highlighted a wide variety of views on whether increased clearing of U.S. Treasuries and repos would materially improve the resilience and efficiency in this market.

Most respondents were broadly supportive of clearing, but there was kind of little support for a clearing mandate. With suggestions that this could lead to participants leading their activities to withdraw from the market, there was strong support for incentives to encourage clearing them.

The SEC has also proposed that clearing agencies offering clearing of U.S. Treasuries should take steps to facilitate access to client clearing. We support the client-based solutions. But it is important that the clearing agencies consult with the market before making any changes to the client-clearing proposals, making sure that the customers have their say.

This will allow market participants to fully understand and prepare for the risks, costs, and benefits of clearing under these proposals.

Before wrapping up, I'd like to bring the committee's attention to the end of the U.S. dollar LIBOR is fast approaching, and the last five settings will cease publication or potentially become nonrepresentative on June 30th. Great progress has been made in this transition to alternative reference rates, but as we enter the final phase, we must not lose momentum. Firms should continue to be proactive and move away from LIBOR and use the tools that are available for legacy transactions.

It's been an honor to provide input on the important and wide-ranging topics of the MRAC agenda. As this agenda continues to evolve, I encourage you to keep in mind and address the both counterparty risk and liquidity risk.

Thank you very much.

CHAIR CRIGHTON. Great. Thank you very much, Scott.

We'd now like to begin a panel discussion on matters relevant to climate-related market risk. The Commission and the MRAC have been active in this space, trying to address the critical matters of the day.

As noted in the agenda, MRAC's Climate-Related Market Risk Subcommittee released a report, Managing Climate Risk in the U.S. Financial System, in 2020. In June of last year, the Commission also hosted a convening on voluntary carbon markets and solicited public comment through a wide-ranging Request for Information.

I'd like to ask Sonja Gibbs, Head of Sustainable Finance at the Institute of International Finance and an Integrity Council board member, to begin the discussion. Following Sonja's remarks, MRAC member Tyson Slocum from the Public Citizen Energy Program will provide a few remarks, potentially followed by an open discussion, time dependent.

Sonja, if you'd begin, please?

MS. GIBBS: Thank you so much to the CFTC and to you, Scott, for suggesting that we join this fascinating discussion.

We very much appreciate the opportunity to give you an update on the work of the Integrity Council for the Voluntary Carbon Market, but I wanted to start with just a quick overview of how voluntary carbon markets are evolving.

When the CFTC held its convening last summer, many of you may remember it was a very challenging time. Issuance was declining. A lot of concerns about oversupply. Ongoing questions about supply side and a demand side integrity in voluntary carbon markets.

Now since then, the picture has improved. Issuance has rebounded. They're still quite small and fragmented, but voluntary carbon markets now at 2 billion USD have quadrupled in size since 2020.

Just to put that in perspective, though, compliance markets have absolutely exploded and are now close to $900 billion, covering almost a fifth of global emissions. So they're still very small, the voluntary markets.

Lots of market building going on. The CME, the London Stock Exchange, CIX in Singapore, Carbon Place, Tokyo. Emirates are launching a big voluntary carbon markets initiative at COP 28 in Dubai. So lots going on.

But to really scale voluntary markets, we need to address two fundamental challenges for market integrity. Specifically, the lack of carbon credit standards and benchmarks on the supply side, and the confusion about how companies are allowed to use these credits to fulfill their climate commitment. So, the demand side of the market.

On the demand side, obviously we've got lots of relevant initiatives. You've got science-based targets, been around for ages, complemented by newer bodies, the voluntary carbon markets initiative, and of course, the work of the Glasgow Financial Alliance for Net Zero, GFANZ, with its focus on transition planning.

We really need all these bodies to be in broad general agreement on the demand side rules of the road for use of carbon credits and in particular to what extent can companies credibly use carbon offsets beyond the purest of removals. For example, avoidance credits that originate in forestry. And of course, our regulators needs to be kept appraised of how these market-led frameworks are evolving, with the hope that this work can be referenced in any future rulemaking, both on the demand and the supply side.

So turning to the supply side, exponential rise in corporate net zero pledges. That's going to mean more demand going forward. Companies are going to need to offset all their residual emissions to reach net zero by 2050, and depending on the estimate, market size could be as much as 200 billion USD by then.

But we've got to address concerns about transparency and standardization in carbon credit markets, and at the Integrity Council for the Voluntary Carbon Market, we are unveiling benchmark standards, these core carbon principles -- the CCPs -- over the next several weeks in two phases. And they're going to set and enforce definitive global threshold standards, drawing on the best science and expertise available. Let me tell you our expert panel of scientists are 24/7. These are very, very dedicated people. And the integrity of supply side credits is going to be very well established in these standards.

So together with an accompanying assessment framework, the CCPs are going to provide a credible and rigorous way to identify high-carbon credits that create verifiable climate impact with high environmental and social integrity and address concerns about permanence, leakage, and additionality.

So, in this context, the recent IOSCO consultation, which we submitted jointly with ISDA, we recommended that securities regulators leverage the work of key governance bodies like the Integrity Council to support greater standardization and strengthen integrity. We think that both securities and financial regulators can use their expertise and authority to enhance market integrity. It's obviously harder on the environmental integrity side.

And important, as ISDA has noted, to clarify the legal classification and regulatory treatment of carbon credits and the nature of actual transactions. For example, in derivatives markets that have a voluntary carbon credit underlying like listed futures or OTC forwards and options.

And finally, there should be continuous monitoring of the development and linkages between compliance and voluntary markets to ensure that as these markets develop, any regulation remains appropriate and fit for purpose. Interoperability of standards is very important here.

So I'll stop here. I know we're short on time.

Thanks.

MR. SLOCUM: Hi, Tyson Slocum, the Energy Program Director with Public Citizen.

First, Commissioner Johnson, just thank you so much for your leadership, and thank you so much for one of the most ambitious agendas that I've ever participated in. I know we're running behind time, but that was inevitable given the ambition of the agenda, and we're really flying through it.

So thank you very much.

So I do think that on carbon offsets, I attended the meeting that the CFTC had, and we offered comments. And the big takeaway there was that there are systemic problems with carbon offsets to ensure that they are verifiable, that they're actually doing what they say that they're doing. And I think what that illustrates is a need for the Commission to take a much more active role in ensuring the integrity of the underlying commodity.

And part of that would be being more proactive, not simply relying on exchanges to come forward with self-certification for products to be listed, but to have the CFTC play a more proactive role in reviewing the integrity of those products. And I think I commend a lot of the actions and efforts by groups to try and come up with better models for carbon offsets, but very often you've got vested market participants that are included in those discussions, which I think just underscores the need for the independence of the Commission to be directly involved in ensuring the integrity of those offsets.

And second, on climate risk, obviously Chair Behnam deserves so much credit for spearheading the creation of the subcommittee and the eventual report that that subcommittee produced. And among the many recommendations was whether or not capital and margin requirements needed to be adjusted to reflect the real climate systemic risk that is posed from climate change. And as part of that also to determine whether or not the CFTC needs to incorporate climate risk into supervisory stress tests of market participants under its jurisdiction.

And so I look forward to the subcommittee being reconstituted as an opportunity to explore these issues more in depth and hopefully result in some rulemakings to get solid rules on the books so that the CFTC can continue to be a leader in ensuring that market participants are protected against systemic climate risk.

And finally, I think that there is a role to talk about position limits. We've got -- finally, after so many years, position limits have been enacted, and I think the Market Risk Advisory Committee would benefit from a detailed briefing of what the Commission's impression of the effect of position limits have been on market functioning, with an opportunity for market participants and others to also weigh in and comment. And I hope that we have an opportunity to talk about some of the other issues that were presented this morning.

The ION cyber attack is obviously just a huge event, and I found it very interesting that immediately afterwards, the Treasury cybersecurity office immediately said there was no systemic risk threat from this. But what I heard today was that there were absolutely systemic risk issues. And in an alternative conference hosted by cyber attackers, they would be popping champagne corks. Because at the end of the day, ION paid the ransom, right?

So it was a successful strategy by the cyber attackers, and part of the reason that ransom was paid was not just because the cyber attack had gummed up the works of derivative markets, but they also had sensitive information about market participants, which I think is a whole other additional market risk issue that wasn't addressed in the comments earlier that I think this advisory committee should explore further. And I'm very glad to hear that the Commission is initiating a rulemaking, and we'll be eagerly participating in that.

Thank you so much.

CHAIR CRIGHTON: Great. Thanks, Sonja and Tyson.

Again, I think in the interest of time, we're going to continue to move forward. So we're going to turn to market structure developments. In particular, today we'd like to focus the discussion on two areas, Treasury market developments and liquidity impacts of recent block thresholds.

We'll hear first from Brian Smith, Deputy Assistant Secretary for Federal Finance at the Treasury. After Brian, we'll hear from MRAC member Bis Chatterjee, Managing Director and Head of Innovation for the Global Markets Division at Citigroup.

Brian, please go ahead.

MR. SMITH: Thank you. And thank you to Commissioner Johnson for inviting me to speak with you today.

I oversee the office at Treasury that's responsible for issuing Treasury securities. I'd like to speak to you about our work to enhance the resilience of the Treasury market.

As you know, the Treasury market plays a critical role in financing the Federal Government, in implementing monetary policy, and supporting the broader financial system. And in recent years, there have been several episodes of deterioration in the functioning of some segments of the Treasury market. Although some disruptions came amid the extreme public health and economic shock at the onset of the COVID-19 pandemic, other disruptions have arisen in seemingly more calm environments.

These episodes underscore the importance of understanding market vulnerabilities and proposing responsive actions. Our efforts are designed to support the Treasury market's ability to absorb and not significantly amplify adverse market shocks that could lead to breakdowns in intermediation. However, we recognize that some shocks can be so extreme, such as the COVID-19 pandemic, and official interventions -- official sector interventions may still be necessary, even with substantive reforms.

In our efforts to enhance the resilience of the Treasury market, we are collaborating across the official sector with the Interagency Working Group on Treasury Market Surveillance, or the IWG. The IWG includes Treasury, the Federal Reserve Board, the Federal Reserve Bank of New York, the SEC, as well as our hosts here at the CFTC.

While we've made significant progress in the last several years, there is still much work ahead. To highlight some of the major recent accomplishments, the IWG member institutions and staffs have proposed policies to enhance the oversight of significant participants in and trading venues for the Treasury market and to centrally clear more Treasury transactions. They've initiated a pilot collection of data on noncentrally cleared bilateral repo and proposed a rule to establish a permanent collection of such data, approved enhancements to the collection and public release of data on secondary market transactions, and begun expanded collection of data on depository institutions' secondary market transactions in Treasury securities.

They've also proposed additional public transparency for Treasury securities transactions that's been informed by public feedback and studied the potential benefits and costs of all call trading in the Treasury market. And finally, analyzed options for establishing more uniform leverage requirements across different market segments and for consistently identifying market participants across data collections.

I want to spend a few minutes focusing more deeply on the data front, which I mentioned briefly. We've begun to collect more information on transactions in both the cash and repo segments of the Treasury market and are actively considering how best to improve the degree of public transparency of that data. This work is intended both to bolster the official sector's ability to evaluate market conditions as well as, we believe, providing additional transparency to the public fosters public confidence, fair trading, and a market ecosystem that's ultimately more resilient.

In 2017, FINRA began collecting transaction data from its members through TRACE and providing that data to the official sector. The release of weekly aggregate volume data to the public began in March of 2020, which coincidentally saw the highest Treasury market volumes on record.

Since then, Treasury has made several -- I'm sorry, FINRA has made several enhancements to the aggregate volume information about Treasury markets and just last month moved to a daily release cycle with additional data elements such as trade counts and average price information. At the same time, Treasury has been considering additional measures to enhance public transparency of secondary market transaction data. We've solicited input from the public that provided a range of opinions on the benefits and risks of enhanced transparency, and based on this input, Treasury believes that additional transparency can provide meaningful and lasting benefits for the Treasury securities market.

To that end, in November, Treasury announced that it supported publicly releasing secondary market transaction data for on-the-run nominal coupons with end-of-day dissemination with appropriate cap sizes. Such data would cover more than half of daily transactions in the Treasury securities market.

As you all know well, the Treasury futures market already has much greater transparency than the securities side, and that's not hampered overall liquidity there. That said, considering the potential risks and the importance of the Treasury market in the financial system, we will proceed in a gradual and calibrated manner.

So thank you again for including me in today's meeting, and I appreciate the opportunity to share an overview of our work on Treasury market resilience and Treasury market structure.

Thank you.

MR. CHATTERJEE: Thank you, Commissioner Johnson, sponsor of the MRAC, to the chair, designated officer and staff of MRAC, for the opportunity to introduce the topic of block trades.

In my remarks, I will briefly touch on the history of block trade frameworks for swaps, the role block trades play in the market, and the importance of monitoring and validating the block trade framework.

Let's take a quick look at the history of block frameworks. Almost 10 years ago, the Commission set up the framework for handling block trades in the swap markets under Part 43. The rules were designed to enhance market transparency and price discovery by making swap transaction and price data available to the public while also protecting the details around identities, business transactions, and market positions.

In the Commodity Exchange Act (2)(A)(13), language was added to ensure that the Commission should consider whether the public disclosure of swap transactions and pricing data would materially reduce market liquidity. The Part 43 framework on handling of block trades hinges on the delicate balance across three factors.

First, determining a size threshold above which a trade will be exempt from prescribed methods of trading or where they need to be traded. Second, the provision for modified public information dissemination rule for time delay. And third, a cap on the size of the trade that is reported.

In 2020, the Commission introduced changes to the block trade framework while giving the market a significant amount of time to make changes to the necessary infrastructure within each market participant firm, set, CCPs, and SDR in order to adopt these changes without creating an operational outage risk.

Moving to the role of block trades. The swap market is comprised of a variety of market participants that are mostly wholesale participants that execute trades in not only diverse capacities, but also vary in size of capital they manage and their risk in investment appetite and strategies. These factors drive their trade execution requirements in terms of the size of the trades they need to execute as well as the time window in which they have to execute these trades.

Given such disparate needs and the nature of the market participants, most over-the-counter markets, including the swap market, do not exhibit continuous and consistent trading participation and price patterns. Added to this, periods of market volatility and economic uncertainty may exaggerate this inconsistency leading to periods of sharp price swings and impaired liquidity formation. It is especially during such periods that block trade frameworks allow wholesale market participants with large trade size needs the ability to seek out the desired liquidity without their specific trade causing further disruptions to the functioning of the market and participants or adversely impacting the execution price or transaction cost of their trade.

At the same time, the block trade framework ensures that adequate information and transparency is also provided to the rest of the market regarding such trades even in volatile market conditions, consistent with the principles of the Commodity Exchange Act and Part 43.

Turning to the topic of monitoring and validation of block trade frameworks going forward. With the ever-changing market conditions and the nature and role of participants, the trade execution needs of marketplaces vary over time. The availability of swap execution data allows the Commission the ability to monitor the trade side price and trading patterns of the participants and gain insights into the functioning of the market, including the efficacy of the block trade framework.

In addition to using simple data analysis like the 50 percent and the 67 percent rule, there may be room to take a look at other important issues that can help enhance the analysis, monitoring, and smooth functioning of the trade execution and price transparency frameworks. Some known areas and questions that can be further addressed are, one, the SDR data reflects historic trading patterns and may not always be the most important factor for current or future marketplace trends. This is especially relevant for widely known and accepted and anticipated events like the migration to SOFR swaps, macroeconomic conditions like central bank interest rate change cycles.

Second, the historic trade data does not distinguish between trades executed during regular market conditions versus those that were executed during constrained liquidity periods.

Third, certain SEFs and regulated trade venues already provide execution methods for transacting block site trades on their platform between participants, and therefore, a significant portion of block trades may already be -- are executed on SEFs and truly not away from the SEFs.

Fourth, should there be provisions for time-limited exceptions to the block trade execution framework, or should there be a fallback to a different threshold for block sizes during once-in-a-lifetime event periods like the COVID lockdown in early 2020 that helps promote continuous liquidity and market functioning?

Before I close out my comments, I'd like to emphasize again the importance of preserving the core principles of transparency and market liquidity. Therefore, in anticipation of expected near-term volatility from widespread macroeconomic conditions, the need to promote wholesale adoption of SOFR swaps, and the scheduled go-live date of the new block framework, the MRAC can play an important role in doing a thorough cost-benefit analysis and assessing the impact of the new block trade framework, especially on participants that today initiate block trades on behalf of their clients and participants that also benefit from the public transparency that is provided.

Thank you.

CHAIR CRIGHTON: Great. Thanks, Bis and Brian. I appreciate the comments.

We're going to head into our final topic for the day, interest rate benchmark reform. We're grateful to have two excellent guest speakers on this important topic, who will update us on transition efforts away from LIBOR to SOFR, as well as remaining transition or implementation milestones.

First, we'll hear from David Bowman from the Federal Reserve, and after that, we'll hear from Nate Wuerffel, Senior Vice President at the Federal Reserve Bank of New York. David, we'll start with you.

MR. BOWMAN: Thank you. I want to thank Commissioner Johnson and her staff for inviting me. I should start by noting that my remarks today reflect my own views, not necessarily those of the Federal Reserve Board.

I should also start by thanking the MRAC for its many years of effort in regards to LIBOR transition and helping the derivatives market to prepare for that transition. Because of many years of effort put in by the MRAC, by ISDA through its work on this protocol, by CME and LCH in the planning for upcoming conversions of cleared over-the-counter and exchange-traded LIBOR derivatives, the derivatives market, which is by far the largest market in terms of exposure to dollar LIBOR, is also by far the most prepared for the upcoming transition.

But, and I need to emphasize this, people still need to prepare and understand what will happen to their derivatives positions as of June 30 of this year. Now large players already have experience with this as part of the transitions of the other LIBOR currencies last year -- 2 years ago. But your dollar LIBOR is by far more widely used, and for many smaller players, this will be the first time they are directly affected by this transition.

We encourage everyone, especially smaller players who will be going through this for the first time, to take advantage of materials LCH and CME have developed and to take part in any practice runs that they may offer. It is also crucial that people make sure that they understand what exactly will happen to each of the derivative exposures.

Uncleared and over-the-counter derivatives held by counterparties that have adhered to the ISDA protocol or that are under U.S. law will convert to ISDA's fallback rate. Cleared OTC derivatives and exchange-traded derivatives will convert to SOFR as well, but on slightly different terms and through slightly different processes than will occur under the protocol, and therefore, it's necessary to understand the differences and how they will take place.

Now these processes are highly efficient and designed to convert a massive amount of LIBOR derivatives to SOFR cleanly and quickly, but they may not be the best fit for every need. In particular, if people have bespoke needs -- for example, to match a hedge to a cash product or other needs that they may have -- it's particularly important that they actively transition rather than rely on these processes.

Now these processes will help to ensure that we safely transition from LIBOR to SOFR. However, we all then need to make sure that we do not repeat the mistakes that were made of LIBOR going forward. Most market participants, in my experience, tend to treat reference rates as something that is semi-magical, numbers that just appear on a screen, and you trade them. And most people don't spend much time thinking about where those numbers come from or whether the uses of those numbers actually make sense.

In many regards, it's sort of the way that I often treat water from a tap. I turn on the faucet, and water appears. I don't tend to think very much about where the water comes from, what the quality is, or if it could ever run out.

But this is real life, and we got into these problems because that is how people treated LIBOR. They traded it. They didn't care where it came from. They didn't care how it was constructed, and they didn't think about the ways that it would make sense to use it or not use it. And as a result, that system has crashed.

The official sector is determined that the same thing should not happen again having had to devote over a decade of work to safely transition the market from LIBOR. In particular, for these reasons, the official sector has clearly emphasized the use of term SOFR needs to remain consistent with financial stability.

Now term SOFR is different from overnight SOFR, which is the basis for the overall transition. Overnight SOFR is derived from the overnight U.S. Treasury repo market, which is a trillion dollar-plus market that has and will exist regardless if anyone -- whether anyone trades SOFR or doesn't trade SOFR.

Term SOFR is based on CME's futures markets for overnight SOFR. Those are active futures markets, but they only remain active if people continue to trade overnight SOFR. Therefore, this transition will only remain tenable if overnight SOFR remains the dominant benchmark.

Now that, again, is not the kind of thinking that most people may have, most market participants. They want to turn on the tap, and they want their term SOFR to come out, and they want to use it wherever they can or for whatever purpose they can. But I think we all need to understand that term SOFR is and needs to remain a limited resource.

For these reasons, the Financial Stability Board, FSOC members, and the ARRC have all strongly recommended that use of term SOFR be limited. Derivatives markets do not need term SOFR. They are functioning at a very high level already using overnight SOFR.

The ARRC has recognized the use of term SOFR in business loans, which is the largest cash product market and includes a very wide range of users of different degrees of sophistication, and the ARRC has recognized use of term SOFR in legacy LIBOR cash products that will fall back, as these are contracts that may have been negotiated long before SOFR or the thought that a LIBOR transition would be needed ever existed.

To support these particular uses, the ARRC has also recognized use of term SOFR in derivatives and some term SOFR securitizations, but only if that use is to hedge or serve these two particular uses -- that is, new business loan activity and legacy fallbacks of term SOFR and cash products. This basic message and this basic framework should not be expected to change. They're a permanent part of the new environment because they have to be.

My fundamental message to people is that we should not be trying to re-create the exact same environment that we have with LIBOR. That environment was not stable, and it crashed. Instead, I encourage people to find new ways to work in the new environment.

In particular, for parties looking to hedge, they should consider all the forms of SOFR, not just term SOFR, and pick the form that is the most cost-effective way for them to achieve the goals that they have.

Thank you.

CHAIR CRIGHTON: Nate, we're ready for you.

MR. WUERFFEL: Thank you. And thank you, Commissioner Johnson, for the invitation to speak here.

I also want to note that my remarks are my own and not those of the Federal Reserve or the New York Fed.

First, I want to thank, as David did, the Market Risk Advisory Committee and the Interest Rate Benchmark Reform Subcommittee, chaired by Tom Wipf, for their leadership, your leadership in the transition away from LIBOR under the guidance of the CFTC.

U.S. dollar LIBOR exposure has totaled over $200 trillion, or about 10 times U.S. GDP, and derivatives made up $190 trillion of that total. So efforts to move the derivatives markets have been critical in reducing the financial stability risks of the transition away from LIBOR.

In addition to the ISDA protocol and CCP conversions, the legacy exposures have been essential to move new activity onto robust reference rates like SOFR. The MRAC's endorsement of SOFR First in the second half of 2021 was instrumental in making this happen, helping the market to move away from LIBOR to SOFR derivatives and interdealer markets, cross-currency markets, nonlinear derivatives, and exchange-traded instruments.

SOFR First was highly successful. We've seen tremendous growth in futures with 2022 volumes and open interest multiple times their level in 2021, and in options multiple thousands of times their levels in 2021. This year, we've already seen record volumes and open interest in both, with SOFR-linked derivatives now the dominant instrument in these markets.

Second, I want to note the importance of ensuring that we never repeat this long, difficult, and risky transition effort again, and the risks to the financial system that it posed. The entire LIBOR transition program has been about moving from LIBOR -- a weak, illiquid rate that is susceptible to manipulation -- to risk-free reference rates, which are underpinned by deep and liquid markets, providing a far more robust foundation for the financial system. Anchoring the financial system in SOFR improves the stability of the financial system, and it's a rate that is underpinned by an average of $1 trillion in daily traded volumes.

It's in everyone's interest to have a sound and robust financial system, and to have that, overnight SOFR needs to remain the primary tool for derivative and capital markets, not term SOFR or other instruments. The official sector has been clear that term SOFR's use must remain limited, in line with the recommendations of the FSOC and the Financial Stability Board, as well as the ARRC.

In a similar vein, it's important that markets avoid falling into the same trap that they did with LIBOR, where something was used as a reference rate for convenience, among other reasons, but was structurally flawed and grew to be a financial stability risk. Robust reference rates should have underlying transaction bases that are also robust through economic cycles and credit cycles as SOFR is. They should not wither up like those based on short-term wholesale bank funding markets that back LIBOR.

Use of robust reference rates like SOFR, adherence to IOSCO principles, and best practices like those of the ARRC should help provide a foundation for a stable financial system over time.

Thank you very much.

CHAIR CRIGHTON: Great. Thank you very much, Nate and David. We appreciate your comments today.

We made it. We're through the agenda. I think what our plan was from here, appreciating the fact that we didn't open it up for any member comments after each of the panels and presentations, we thought we'd pause now and actually open it up for those comments and feedback.

Appreciate it's been a long morning. There's been a lot of content that we've discussed. So in the event that this format doesn't work, we can review other ways to provide that feedback as well.

And good timing. So we'll open it up for some comments now. As a reminder, if you would turn your placard to the side so we can recognize any comments you'd like to make.

I recognize Bis.

MR. CHATTERJEE: Thank you.

Just maybe turning to Dave and Nate and your comments on term SOFR and the adoption, how do you see the role of banks, dealers, various marketplaces in kind of like the use of term SOFR? Stay away from them? Adopt them where it helps facilitate overnight SOFR? So would just love to get your opinion on that.

MR. BOWMAN: Yes, so the ARRC has made recommendations, best practice recommendations around use of term SOFR versus overnight SOFR. Some of those recommendations are already reflected in some of CME Group's license, though not all at this stage. And of course, the official sector has late last year and this year kind of emphasized their commitment to the spirit behind those best practice recommendations.

So I think banks and dealers, certainly after the official sector messaging, if not before, do take the best practice recommendations fairly seriously at this moment. We do understand that not every deal involves a bank or a dealer and that some of the ARRC best practices recommendations like, for example, if you're using the term SOFR derivative, it should be to hedge a term SOFR cash product or not things that a dealer can naturally police with full satisfaction, right? They can remind people of the best practice recommendations, ask for statements that people intend to follow them, but they can't police every aspect of it.

So I think banks and dealers do play an important role in helping to keep use of term SOFR limited. I think at this stage, they do understand the importance that the official sector places on them, but we can't simply rely on them because SOFR and term SOFR are used across -- across the market. And therefore, (inaudible) encouraged CME Group to consider embedding more or all of the ARRC's best practices into its license agreement, which could also help keep use of term SOFR limited.

MR. WUERFFEL: Maybe I could just add briefly to what David said and pointed out so very well? When the ARRC thought about term SOFR, obviously, the guidance globally has been to use overnight risk-free reference rates as the basis for transitions given the robustness. But the ARRC recognized that there are some parts of the market that might have more difficulty transitioning away from U.S. dollar LIBOR, and that particularly the long markets posed that challenge.

And so term SOFR in the first instance was thought of as a narrow solution for loan markets. But of course, to make that effective, you also need to be able to hedge some of those risks associated with that. But there is this sort of bright-line best practice, which is not to use it in interdealer derivative markets, where, once you begin interdealer trading, you could imagine that the volumes of term SOFR derivative transactions could grow very rapidly.

And of course, as David pointed out earlier, term SOFR itself is dependent upon not term derivative transactions, but overnight derivative transactions. And so you would not want a situation where the use of term derivatives and derivatives markets actually cannibalize the use of overnight interest rate derivatives based on SOFR. And so I think that that restriction, that best practice not to use it in interdealer markets, along with the other recommended limitations on the scope of use, are incredibly important.

And I do think it's been very helpful to have these begin to be reflected in the licensing and also that market participants have widely been looking at and adopting those best practices that ARRC has recommended to make sure we don't run into a financial stability problem where we've hollowed out the very thing, the very transaction base that makes up term SOFR.

COMMISSIONER JOHNSON: I'm going to exercise a bit of sponsor privilege here, and notwithstanding the fact that, David, you've offered one of the most colorful and enjoyable illustrations I've heard at all in the context of interest rate benchmark reform in the context of turning the water on, the faucet on, the tap. I wanted to just emphasize, because I think our chair sort of opened the floor in this moment, but we really are sort of thoughtful if there were comments from earlier in the program that we should just take a few minutes and hear those comments.

We know how precious your time is and also how important it is when we come together to hear those diverse viewpoints, to get them on the public record, and to make them part of the discourse. And so we acknowledge this, today's MRAC meeting is a little bit different than our conventional approach, and we anticipate going forward for the rest of the year, there will be -- we'll be much more engaged in conversations that probably started in other spaces and are coming to fruition here. But we don't want to miss the chance to hear from you if there was something earlier today that you wanted to comment on or share about.

We certainly anticipate continuing conversations on every topic we touched upon here, but throw the doors open. And Ernie, I'd happily like to start with you, if that's okay?

MR. KOHNKE: Thank you, Commissioner Johnson, Chair Crighton, and everyone who is helping with this event.

I'm Ernie Kohnke. I'm here on behalf of Commodity Markets Council. I'm the General Counsel for the Americas for Vitol.

Many people know Vitol for its traditional businesses, but Vitol is also investing in developing sustainable initiatives, including environmental products, renewable energy, and related activities. We currently have 1.2 gigawatts of solar wind projects. We're implementing circular economy solutions to include plastic and tire cycling. We're working on a full decarbonization project for one of our UK power plants that will remove 8 million tons of carbon dioxide, eventually switching to full fuel from hydrogen.

And so I particularly found it helpful to hear from Ms. Gibbs and her efforts to establish firm framework for what the terms are for the various products that underlie the voluntary carbon market. Vitol transacts in these voluntary carbon products, and in our view, most of the deals right now are still being negotiated over the counter largely because the markets have not coalesced around a single standard for environmental credits.

The exchanges, however, are continuing to develop new futures contracts for environmental credits, and the open interest in those contracts is continuing to grow. Also, as was mentioned before, ISDA has published its definitions and template confirmations for use with environmental products. I think both of these efforts are going to be very helpful to bring stability to the market.

But as we negotiate these transactions, we are seeing three kind of core issues that is making market participants a bit uncomfortable with the risk associated with transacting in these markets. The first is additionality. Many companies, of course, are only willing to contract for what they view as an additional contribution to either carbon offsets or carbon removal, but there is just not clear guidance or market consensus on what that means.

And an example of what we've seen in some of our discussions is with respect to wind farm, if it is repowered, is it the additional output that therefore only qualifies for additionality? And it's a particularly difficult concept in the carbon space when you're not looking at just removal projects, but also avoidance projects as well, like afforestation or cookstove projects in particular.

The second, of course, then follows on from that, which is the legitimacy of credits and the potential for double counting. Many of the carbon avoidance projects are localized and managed by local groups and NGOs, which then creates a certain lack of transparency, and certification continues to be a problem as many interested players remain concerned about that legitimacy. And I'm glad to hear that the Integrity Council is really focused on that element, which we think is foundational for the development of these markets.

Another related concern is just the tagging and tracking of the credits themselves and the retirement obligations and what happens if the party that committed to retire those credits does not.

And the third main risk that everyone is very concerned about is the risk relating to greenwashing. And of course, Chapter 7 of the MRAC's September 2020 report does an excellent job explaining the benefits of accurate climate-related financial disclosures and the value to that and provides 12 recommendations in particular to promote those accurate disclosures. In today's market, however, the risks associated with making public statements is creating confusion among the people who are transacting in these credits.

Again, the underlying products don't have those core standards that we would need to rely on for those public statements. It creates liability risks from shareholder actions or enforcement actions from regulators. We are seeing increased focus on following the Federal Trade Commission Green Guides, but again, those provide a broad framework that really doesn't eliminate the risk.

So, anyway, I just wanted to take the opportunity to lay out what we are seeing in terms of the actual transactions in these markets in the over-the-counter space, and thank you for the opportunity.

CHAIR CRIGHTON: Thank you for that feedback. I think we'll go ahead and look to conclude the meeting.

So, first, I'd just like to say thank you. We're incredibly thankful for the insights of all of our guest speakers today, as well as the thoughtful contributions they've made. I think the detail and the preparedness of what was provided today was extraordinary.

So, thank you.

I'll turn it over to Commissioner Johnson to close us out.

COMMISSIONER JOHNSON: Yes, thanks so much, Alicia.

I'll share the following. Certainly an ambitious menu, if you will, of issues. Really intended to get your wheels turning.

What I'd like to share in advance is a bit of a call to action for the MRAC members who are serving on the main committee. Our expectation is that you will take up the mantle as with respect to some of the issues that were raised here and that you will raise your hand and volunteer to support the subcommittees, the workstreams that they will undertake, and possibly even offer yourself up for leadership.

Thanks, Ann Battle, so much for that.

All right. So, essentially, our goal is to ensure that everyone is serving in a particular space, and ultimately, it's somewhat helpful, I think, if folks leave today's meeting with some thoughts about where we could most use the talents and expertise that you have. We certainly have been thinking about this for the last few months, and now we're hoping to put our shoulder to the plow and ask you to do the same as we really begin to dig in and dive into some of the issues that were presented here and develop workstreams that really are consistent with the successful projects that have been launched and that have led to the creation of proposed rules and adopted rules integrated and implemented by the Commission.

So we really are hopeful that today's very demanding schedule and very demanding intellectual engagement triggers thoughts about how you can participate directly going forward in the workstreams of the various subcommittees. And if there are issues that we didn't think about that really ought to be at the core or the center of MRAC's discussions, please do follow up with Bruce or Marilee. We would love to try to in the very least channel those topics and those issues to the subcommittees who will, acting on their own authority, really take those issues up and run with them.

We're grateful for the time you gave us today. It's our most precious commodity in most instances. So we really do want to thank you for that, for your talent and your expressions and expertise.

I think Bruce has to say some official words to close out the meeting, but we're grateful for all of you who were able to stay on and apologetic for those who may have been delayed in transitioning to trains or the airport.

Thank you for being here.

MR. FEKRAT: All right. Thank you, Commissioner. Thank you, Chair Crighton. And I also want to thank all the members. And Walt, thank you so much for being here.

And thank you, everybody, for attending our first MRAC meeting of 2023.

The meeting is now adjourned.

(Whereupon, at 1:07 p.m., the meeting was adjourned.)