COMMODITY FUTURES TRADING COMMISSION

TECHNOLOGY ADVISORY COMMITTEE

(TAC)

10:00 a.m.

Thursday, October 3, 2019

CFTC Headquarters Lobby-level Conference Room

1155 21st Street, NW, Washington, D.C. 20581

TECHNOLOGY ADVISORY COMMITTEE (TAC) MEMBERS

Richard Gorelick, Chair
DRW Holdings, LLC

Erik Barry
Credit Suisse

Christopher Chattaway [via telephone]
Goldman Sachs

Thomas Chippas
ErisX

Charley Cooper
R3

Gary DeWaal
Katten Muchin Rosenman LLP

Christopher Hehmeyer
Hehmeyer Trading and Investments

Mayur Kapani
ICE

Derek Josef Kleinbauer
Bloomberg

Brian Knight
Special Government Employee (SGE) for CFTC
Senior Research Fellow, GMU Mercatus Center

Brad Levy
IHS Markit

John Lothian
John J. Lothian & Company, Inc.

Timothy McHenry
National Futures Association

Lee Olesky
Tradeweb

Alexander Stein
Two Sigma Investments, LP

Larry Tabb
TABB Group

Supurna VedBrat
BlackRock

Yesha Yadav
Special Government Employee (SGE) for CFTC
Professor of Law, Vanderbilt University

A G E N D A

A G E N D A

A G E N D A

A G E N D A

A G E N D A

Page

P R O C E E D I N G S

(10:00 a.m.)

MS. TENTE: Good morning. As the TAC Designated Federal Officer it is my pleasure to call this meeting to order. We are very much looking forward to today's presentations.

Three logistical items before we begin. First, please push the button on your microphone to speak, the red light means the microphone is on. For those participating by phone, please keep the phone on mute until you are ready to speak and introduce yourself before speaking. If you'd like to be recognized during the discussion, please lift your name tents so the Chair of the meeting can recognize you and give you the floor.

Chairman of the TAC, Richard Gorelick, will lead the meeting today, but first Commissioner Quintenz will give his opening remarks.

COMMISSIONER QUINTENZ: Thank you very much, Meghan, and good morning to all of our distinguished members. Thank you very much for your participation, your willingness to be here, your contributions to the

committee and to all of our subcommittee members who are not on the full committee, let me also extend a very warm welcome to Chairman Tarbert for his first Technology Advisory Committee meeting. It's great to have him here. I hope he finds them as informative and engaging as I have over our last three meetings, I don't think this will disappoint.

And thank you, Meghan, for your tireless work. Meghan is our Designated Federal Officer and has worked very hard to make today robust and seamless. And let me also as always, thank the hard work of our subcommittee DFOs, John Coughlan, Scott Sloan, Phil Raimondi, and Jorge Herrada.

Forgive me for some extended opening remarks, but I think we have a number of very important issues to talk about today that I think there's either lack of clarity on generally because of the nascency of this space or things that we've talked about for a long time on which I have strong views, but starting off we have what I think is going to be an interesting presentation by our Virtual Currency Subcommittee that's going to hear from Gary DeWaal, Special Counsel

at Katten, and Lee Schneider, General Counsel of block.one, on the key characteristics and legal treatment of stablecoins.

And although the definition of stablecoin is evolving, I think currently, they are generally thought of as a class of virtual currencies that seek to offer price stability or at least a value floor by being backed by price stable reserve assets. Because they strive for price stability, stablecoins have the potential, I guess, in my opinion, through tokenization, to function as a viable and liquid medium of exchange. But given the nascency of this class of digital assets I think it's important to approach any stablecoin consistently with other products that have similar characteristics, mechanics, and structure.

We should not be trying on fit a square peg into a round hole, but if something is a round peg it needs to go into a round hole like everything else. So I hope that Gary and Lee can give us advice on what's square and what's round.

Next the subcommittee is going to hear from Dr.

Chris Brummer, Professor and Director of the Institute of International Economic Law at Georgetown, and Tom Chippas, the Chief Executive Officer of ErisX, to discuss some of the unique challenges associated with cryptocustody. The protection of private keys by cryptotrading platforms, trust companies, clearinghouses and others is an evolving landscape, best practices which have quickly become robust. We're going to hear from our Distributed Ledger Technology Subcommittee that’s going to presenting on some real world applications of DLT technology, including with respect to custody and collateral management. I think DLT holds great promise to safeguard individual’s privacy, promote data integrity, and ensure confidentiality.

As the technology matures I think it's going to be interesting to explore whether there's a role for DLT to play, with respect to firms demonstrating their compliance with CFTC record retention requirements, for instance, specifically if the agency could ever at some point over a blockchain and through something like a zero knowledge proof verify that certain

records exist within a firm and are being maintained appropriately, that process could significantly enhance customer protection, promote regulatory compliance, while not requiring enormous regulatory resources or exposing sensitive data to cyber risk through electronic transfers.

Our Automated and Modern Trading Market Subcommittee is going to continue its examination of the true risks inherent in the modern trading environment, and whether or how those risks are currently being mitigated. In my view, many of the risks posed by automated and algorithmic trading are being addressed through market incentives, including exchanges in firms' own self-interest to limit significant operational risk to their businesses.

But to the extent gaps may exist, it's been my hope the work of this subcommittee can illuminate them and begin a conversation about the best way to examine them and solve them.

Prior TAC meeting presentations and discussions have already added a lot of clarity to that landscape. To refresh everyone's recollections, in a prior TAC

meeting we had Bryan Durkin with CME Group to present on how CME has implemented trading and volatility controls that complement, and in some cases exceed, the eight recommendations published by IOSCO regarding practices to manage volatility and preserve orderly trading.

More recently, the CFTC's Market Intelligence Branch presented its own research report entitled, “The Impact of Automated Orders in Futures Markets.” You know, that report contained several significant findings, and although they’re general and preliminary, it included that the increase of automated order activity generally seen across all commodity markets has not correlated to increases in end-of-day price volatility and actually in some cases that the volatility declined as automated trading increased.

Building upon that work, we're going hear from Alicia Crighton, a Managing Director of Goldman Sachs, who will discuss FIA’s best practices for exchange and firm risk controls. FIA has played a critical role in advancing risk management and trading controls through

development of these best practices, and their subsequent industry surveys regarding those best practice adoptions. Ms. Crighton will discuss current pre- and post-trade risk controls being implemented by exchanges and firms today, taking into account the dynamic and ever-evolving nature of these controls. She will give us a preview of some of the next generation of controls and best practices that are currently being developed by exchanges and firms to further refine and improve electronic trading systems and protect integrity of our markets.

Next, and directly supplementing the prior TAC's meeting presentations by CME, Mayur Kapani the Chief Technology Officer for the Intercontinental Exchange, will present on the risk controls that ICE implements across all of its markets. Mr. Kapani will also walk us through a real life example illustrating how these risk controls worked during the recent volatility spike in Brent.

Both of today's presentations demonstrate to me how trading and risk management controls continue to evolve with the trading technology itself. Controls

are constantly being updated to improve and respond to market developments. Given how quickly advancements in risk controls are occurring, I'd be curious to hear from the subcommittee and the full TAC if it would be informative to have an updated analysis to determine what best practices look like in 2019 and how widely they have been adopted.

Finally, the Cybersecurity Subcommittee is going to present on the Financial Services Sector Coordinating Council, or FSSCC Cybersecurity Profile, building upon the overview provided at our last meeting. Following that presentation the subcommittee would like to discuss with the full committee whether the TAC should vote to recommend that the Commission issue a statement of support for the FSSCC Cybersecurity Profile at the next TAC meeting. I'm interested in hearing the feedback from the full committee on that.

We'll also hear from Jason Harrell, the Executive Director and Head of Business and Government Cybersecurity Partnerships at DTCC regarding vendor risk management. Mr. Harrell will discuss some

challenges of effective vendor risk management and some potential alternative approaches that may address those challenges.

Before I conclude, I would also like to thank Richard Gorelick, TAC's Chairman, who is also the chair of one of our subcommittees and member of another subcommittee, for his tireless work in preparation and advice in putting today's agenda forward. Thank you all and I will turn it back to Meghan.

MS. TENTE: Chairman Tarbert, would you like to make some remarks?

COMMISSIONER TARBERT: Sure. Welcome, everyone. Thank you all for coming, especially thank you to Commissioner Quintenz and his staff for convening the TAC. I would also like to thank you, Meghan, for your work and being the DFO for this committee and also to Richard Gorelick, of course, for chairing the TAC, and all of you for traveling from far and near to come here to the CFTC to take the time to share your valuable perspectives.

This advisory committee in particular has a vital

role to play in the operation of our agency. We regulate markets that are at the cutting edge of technological innovation. As an agency, particularly a federal agency, we don't always have the technical expertise that our market participants have. We can keep pace with our markets only through a dialogue, an active dialogue, with those in the markets and all of you who are driving these developments.

The topics for today's meeting reflect the rapid technological transformation taking place in our markets, automated trading systems, stablecoins, and digital assets, DLT, cybersecurity, and the other topics that Commissioner Quintenz mentioned. These are exactly the types of issues we must gain insight from industry. Our interest in these issues stem from our larger mission, our job is to ensure that our rules protect market integrity while fostering innovation. And in fact, if you go to the CEA, the Commodity Exchange Act, the word "innovation" actually appears in the statute itself in the history and the purposes. And I think that's really unique to the CFTC.

But that, of course, requires a bit of balancing act at times, market integrity as well as fostering innovation. Market integrity is obviously about protecting customer assets, making sure that our markets function, and making sure everybody knows the rules. If our markets are good enough, there's no need to fix anything. But good enough isn't it the ultimate objective and it never has been for the U.S. financial markets. Our markets are always striving to improve.

Now fostering innovation on the other hand, as opposed to market integrity, is about letting change happen in order to find a better way. But as all of you know, perhaps more so than even us, innovation can be messy. Some innovations are a dead-end and don't live up to their promises. Other innovations create more problems than they solve. And any innovation can take a long time to realize its potential. Innovation also sometimes bears risks. If the new mouse trap is better at catching mice but ends up burning down the house, then it's not a better mouse trap.

So how can a regulator strike the right balance

between maintain the integrity of the system while fostering innovation?

Well, fortunately for us, the best way to strike this balance, in my view, is through a principles-based approach to regulation. And that has been a hallmark and I would argue a very unique feature of the CFTC's regulatory regime. We can set destination but we leave it to our registrants to find the best path to get there. This approach allows flexibility for our markets to take advantage of new technology and other advances but still retains fundamental regulatory mandates so everybody knows what's expected of them.

If we the regulator can better understand innovations in our markets, then we can make sure we have the right balance of principles and rules that actually strike that balance that I mentioned.

So, I very much look forward to hearing all of your views on these important issues. I may not be able to stay for the entire meeting but I've got the Power Points and I've got the video, and so, sometimes late at night on the weekends, I find myself watching

these advisory committee meetings and in fact, sometimes more than once, so I really feel like I understand all the great things that you're contributing. So thank you so much for having me. It's an honor to be here.

MS. TENTE: Thank you, Commissioner Behnam.

COMMISSIONER BENHAM: Thanks Meghan. Good morning everyone. Great to see all of you back in Washington. I want to give a special thanks to Commissioner Quintenz, thanks to Meghan and Richard for your leadership here and it's great to see everyone, packed agenda, I look forward to hearing some of the findings and the work that you all have been doing over the past few months and working with all of you in the weeks and months ahead. So thanks again.

MS. TENTE: Commissioner Stump.

COMMISSIONER STUMP: I have no formal comments, but thanks to everyone who worked to pull this meeting together. Thank you.

MS. TENTE: And Commissioner Berkovitz.

COMMISSIONER BERKOVITZ: Thank you. And I'd like

to echo all the thanks and appreciation to Commissioner Quintenz for sponsoring the meeting, for Meghan for facilitating it, and Richard for chairing it. And I thank all the members for your time and energy, what I know is a volunteer effort, and taking time out of your schedule to help advise the Commission on these important technical issues. I look forward to all the discussions today on crypto, distributed ledger, cybersecurity.

I want to take this opportunity to mention very briefly another technology topic, using infrastructure technology to make regulatory compliance more effective and efficient. Regulators and market participants have accomplished a great deal in implementing the post-crisis regulatory reforms, these have resulted in a safer, more robust financial system. However, we can improve on our accomplishments and I believe technology will be an important driver in our efforts.

Compliance with the new regulations has not been perfect. Just this week if you've been watching our website, the Commission announced numerous swap

reporting violation enforcement actions, aggregate penalties for swap reporting violations are now in the tens of millions of dollars, over $30 million and counting. And this is the amount we have assessed. It does not include the millions of dollars spent on lawyers and consultants to address and remedy these violations many of which could have been avoided with better technical solutions to begin with.

It is my belief that FinTech solutions, that digitize and automate swap transactions and life cycle events, will lead to compliance that is both more complete and more cost effective. The benefits of automation are realized when repetitive processes are standardized, digitized, and automated. Consistency will reduce errors and human input, improving level of compliance over millions of swaps.

In addition, integrating compliance features into transaction infrastructure will increase compliance rates and the public benefits of regulation are more likely to be realized. While much of the substantial cost savings from digitization, automation, and standardization will relate to transaction costs

generally, savings and compliances costs can also be expected. These savings will be passed on ultimately to end-users in our markets, resulting in lower transaction costs.

The CFTC can and should play a significant role, working with market participants and FinTech providers to help them build automated solutions that are cost effective in fulfilling regulatory requirements. To the extent feasible, and permissible, the CFTC should also be more mindful of the role of technology and compliance and take further steps to integrate technology considerations into its approach to regulation. Engaging with FinTech developers and market participants on integrating compliance into technology solutions should be a routine part of CFTC's work.

If we can do this successfully, the CFTC will have helped the industry achieve more effective and efficient compliance. This is a win-win for the CFTC and derivatives industry.

Thank you again and I look forward very much to today's presentations.

CHAIRMAN GORELICK: Thank you. Commissioner Quintenz, Mr. Chairman, Commissioners, and everyone participating today. The TAC is an important venue to foster public dialogue on the role of technology and automation in today's modern electronic markets. The TAC subcommittees have spent the past months discussing technologies and developments that have important impacts on the markets.

I look forward to facilitating the TAC’s discussion today to assist the agency in continuing to promote a regulatory environment that understands and utilizes technology to encourage fair competition and innovation, and to give the Commission the tools to continue to be an effective modern regulator.

With that let's turn to the first panel, which will include two presentations from the Virtual Currencies Subcommittee.

First, we'll hear from Gary DeWaal, who is the Special Counsel and Chair of the Financial Markets and Regulatory Group at Katten Muchin, and Lee Schneider, General Counsel of block.one. Gary and Lee will present on stablecoins and the potential implications

for regulation. Thank you.

MR. DeWAAL: Thank you, Richard. Thank you, Commissioner Quintenz and thanks to all the Commissioners and their staff and Jorge who literally whips us every day to ensure that we are here and making, hopefully, valuable presentations. It's an honor.

So, as way of introduction, if you don’t know me I’m the Gary DeWaal they referred to and this is Lee Schneider. And we're here to talk about, as you said, stablecoins.

In general, I agree with Commissioner Quintenz's definition and I’d like to expand a little bit more though. Rather than just being crypto assets, that endeavor to maintain a stable value against a basket or individual assets, I’d like to talk about stablecoins being crypto assets that endeavor to maintain a stable value against a target referent. Lee will tell you, in a few seconds, that a referent can be tangible or intangible and the means of achieving stability can be quite varied.

I will tell you the Devil is in the details as

far as what the construction of stablecoins are because an analysis is critical to determining how and which regulations might apply. But even though it's critical, and even though it's helpful, it's far from certain, even after analysis which regulations might apply.

Currently there are 65 to 70 active public stablecoins, there are also virtual assets effectively -- that are private and are effectively like stablecoins. One stablecoin, Tether, is currently the fourth largest cryptocurrency by market cap, after Bitcoin, Ether, and XRP. At the end of last year, the market cap of stablecoins was three billion, and of course, there's Facebook Libra.

Here to provide more insight into the nature of stablecoins and to discuss -- is Lee, and then afterwards I'll discuss the regulatory environment.

MR. SCHNEIDER: Thank you Gary. Thank you to all of you on the committee. It's a pleasure and honor for me to be here and talk about some of my views on stablecoins, and I'll emphasize the point that these are my views, I'm not purporting to speak on behalf of

block.one or anybody else.

Let's take a step back before we dive into the topic of stablecoins, and just remember that with respect to any crypto asset, what we're talking about is digital representation. And you live in a world of digital representations all the time, so it's important to remember that crypto assets are just another form of digital representation.

What do I mean by that? Well, when I shop for shoes in a shoe store, I actually pick up shoes and I hold them and I try them on. When I shop for shoes online, I look at digital representations of shoes. Now you could posit a stablecoin that is effectively a digital representation of a shoe, and before you all say that's ridiculous, let’s think about the market for sneakers. There are lots of people who buy and sell rare sneakers with the expectation the value of those sneakers is going to go up. And many of those marketplaces are in the virtue virtual world and may not rely on cryptographic encryption on a blockchain, but there’s still digital representations. So you could you have a stablecoin that’s equal to a pair of

Yeezys, shoes that I know nothing about other than the name.

Another way to think about stablecoins is what else can you digitize and create as our digital record? You can -- as many blockchain companies are talking about, think about identity, as on the blockchain. In other words, a blockchain asset that is representative of people's identity, and with apologies to my psychiatrist, I like to think I'm stable, and so my identity should be fairly stable and would be a form of stablecoins.

My point here is we need to really, as Gary emphasized, focus on the functions and features of the stablecoin, or frankly, any other digital asset that we're talking about. And when I look at the world, at least from a legal standpoint, I sort of see two categories of assets: physical assets, or tangible assets, and intangible assets.

And stablecoins are often designed to be stable against the value of the referent asset, the underlying -- in some cases underlying asset, in other cases referent asset, and that underlying asset can be

a physical asset like gold, for example, you could have a stablecoin that equals one gold coin minted by the U.S. Mint, but it could also be intangible assets like dollars, like securities.

What are intangible assets? Intangible assets really are human ideas or concepts that we give a legal wrapper to in order to consider them to be assets. And stablecoins are just providing a digital wrapper around that legal wrapper so that you know what the referent asset is.

With physical assets stablecoins, if it's a direct link like my example of the U.S. Mint gold coin, I think really that's no different than the situation of shopping for shoes.

With regard to intangible assets it often gets a little more difficult because you've created a digital representation of that intangible asset, but how have human beings done that in the past? Well, human beings have used, for example, paper stock certificates to represent shares of stock. They've used dollar bills to represent USD fiat currency. And using a digital representation of those things really

isn't designed to change the character of it.

I like to joke with people that there has long been a U.S.D. stablecoin, it's called a bank deposit account, right? It’s a digital representation; I access my bank account on an app, and regularly transact through the app in U.S. Dollars, none of which is currency at all -- physical currency, at all.

We live in this digital world already and what the people who are creating stablecoins are trying to do is mimic a lot of the ideas that we are already implementing in the world, just using the power of blockchain and encryption to try to make them a little bit more transparent, and a little bit more auditable and safer.

So, when I look at these issues, I really feel that by digging into the functions and features of the stablecoin, that is what gets me to the point where I can do some legal analysis about it, and gets me to the point where as a securities lawyer, I can have good debates with Gary, who’s a futures lawyer, and we can try to untangle, are we dealing with something that's future/swaps world? Are we dealing with

something that's securities/security-based swaps world? Or are we just dealing with sneakers?

So, with that I'll turn it back over to Gary, who's going to talk more about the legal analysis.

MR. DeWAAL: Yeah. So, to me, and thank you. I don't know why, as you were speaking, I remembered my first class in philosophy, and Descartes, remembering that when I look at things I don't see the thing. I see the image of the thing. So, I guess the concept of stablecoin has been around a lot longer than I had anticipated.

The legal analysis of stablecoin, to me, is fascinating and it's based upon a statement I've made many, many times, which is, the whole regulation of virtual assets is complicated not because they are a new asset, but because the evolution of regulation generally which was mostly developed in the financial services industry in the early 1900s, 1920s and 1930s, has evolved and over time because of the way it's evolved and because of the way that financial instruments have evolved, there's been a mismatch between regulation and the instruments themselves.

And what the whole aspect of virtual assets have done is they have amplified that problem. So that nothing neatly fits in.

But a lot of the problems that we're dealing with in the virtual asset space really preceded the advent of virtual assets. For example, as I say, everybody remembers the 21(a) SEC report on the Dow, but in fact, the SEC's 21(a) report on Eurex Deutschland would be more interesting, to me, because it showed one day something could be a basket of securities and be regulated by this agency exclusively and the next day it could be something else regulated by the SEC typically because the market cap of one of the components had changed. And you've seen that.

So what's the issue with stablecoins? What is the problem? Well, I think as Lee has pointed out, stablecoins are simply another electronic manifestation of something. You know, there have been gold warehouse receipts for a very, very long time. No one really necessarily needs to touch a physical receipt anymore. People pass the electronic warehouse receipts. And they generally have been dealt with as

traditional warehouse receipts applying whatever the traditional requirements might be.

It shouldn't be any different for these new instruments called stablecoins simply because of what they are called, simply because they are called -- they are a form of virtual asset. And that's why it's important to look into the different types of stablecoins, and figure out what they may be.

So obviously, there are the stablecoins that are singularly backed by an individual something, whether it's a currency, or an asset. Tether, for example, being backed by theoretically U.S. Dollars, and Paxos Gold, for example, being backed by a kilo of gold.

The construction is very, very critical. If a stablecoin is backed by a single asset so that there's no override of management involvement, it's someone gives the dollar, it goes into a custody account, a stablecoin is burnt that effectively reflects that one dollar. First of all, the value of a stablecoin allows you to transact on the blockchain potentially with something that has stable value. A merchant who is used to thinking in U.S. Dollars is much more

inclined to take a stablecoin for payment than Bitcoin whose price may vary rapidly.

If something is backed individually by a single dollar or a single gram of gold, then certainly one could argue it is not a security. Certainly the Howey test, the traditional Howey test does not apply. There is a question because everybody knows about Howey, there's another famous SEC decision, known as Reeves, and that involves whether an obligation of the issuing firm might constitute a security. And typically there's a presumption that an obligation instrument of a corporation is a security, unless it has a family resemblance, that's what the Supreme Court said in the 1990 decision, to things that are not securities. But if the purpose -- as in that case, where there was a bankruptcy of a farmers cooperative, and the allegation against the accounting firm, which was that you did not apply GAAP in the way you accounted for this product, and if you had applied GAAP we would have known that the company was going to be insolvent and the 1,600 people who lost an aggregate $10 million, theoretically, would have had

better notice.

Well, what the Supreme Court basically said is apply the four tests. What was the purpose of the obligation? Was it -- in this is case it was capital raising, that’s what it seems, that’s how it had been marketed. What was the plan of distribution? In Reeves, it was wide spread and it was a public sale. What was the reasonable expectation of the public? In Reeves the Supreme Court said that people were buying it as investment. And is there something else out there that would have provided regulatory protection? And again, the Supreme Court said in this case the answer was no. So none of the components that might have shown that it had, you know, an exception to a resemblance to securities was at play. So a decision was made that it was a security. That analysis could lead to an individual coin under stablecoin with one asset under some circumstances, in my view, likely being deemed a security but where there is dedicated custody of something and the claim is really against that custody element, I don't think the Reeves test is met. But a slight permutation can change things.

So for example, where stablecoin today might be backed 100 percent by USD, but tomorrow be backed 70 percent by USD and 30 percent by an IOU or something else. Then maybe Reeves does become relevant - - maybe Reeves does become relevant - - and maybe something that today was not necessarily a security, like in the Eurex Deutschland order, tomorrow is. That's potentially a problematic outcome.

Moreover, if it has multiple instruments backing the stablecoin and somebody is in charge of deciding what those multiple assets are, and what percentage those multiple assets need to be, in order to achieve the stable price -- well, maybe now you're back into Howey-land, maybe you're relying on whoever is making that decision to manage the assets. Maybe you are in collective investment vehicle-land. I mean, as you start permutating facts, you can start moving in different classification lands with different outcomes. And this is just the United States. And this is just looking at whether something is a security or not.

There are other regulators that are relevant to

the process, as there are with all virtual assets.

If something is of the nature of a virtual currency, then likely - - and there's an issuance of a virtual currency, it is potentially likely that the issuer falls in state-land under the money transmission regimes. It could be deemed a payment issuer. The coin itself could be considered a payment instrument. The transactions on an exchange likely also fall within the money transition regime. Why is this relevant and why is it also relevant also at the fed level because now you’re talking FinCEN BSA, the Bank Secrecy Act, AML requirements.

You’re talking the same things at the state level, but you’re also talking about other necessary registration requirements. In New York State you're talking potentially Bit license.

There are a host of different permutations and there's some things that necessarily fall within the cracks. The OCC recently tried to develop a FinTech licensing authority, it was challenged by the Department of Financial Services in New York and some other state regulators. And ultimately, we'll get a

decision now on that. As regulators fight over turf in this space, as to who regulates.

And there are issues out there that haven't even been discussed. At least in any formal intellectual way. One could argue, and I don't think they should, but it has been raised that the definition of a swap under the Commodity Exchange Act is so broad, so broad, is it possible that a stablecoin could fall within the definition? It's a call, or similar option of any kind, for the purchase of sale, or based on the value of a commodity, maybe. It's been raised. I don't think that's the right outcome.

But the issue is, is that this is a continuum. Stablecoins represent a continuum. They are all objects based on some referent. That referent could be an asset, a tangible asset, sneakers. It could be something more intangible, or it could be an algorithmic device that maintains stability through the process of the algorithm. Once stablecoin has withdrawn, even though it's achieved $133 million in private equity financing, Basis, because the indication was their method of algorithm was likely to

be deemed a security or an investment contract -- make the whole process an investment contract by the SEC, they didn't want to go forward.

Little permutations can have great differences, and that's just the United States. Regulators around the world are formally studying this, partly because of the proposed introduction of Facebook Libra. Earlier last month, FINMA, the Swiss regulator, came out with guidance on stablecoin.

Interestingly, their basic proposition, is they were going to apply a principle of same risks, same rules. No matter what we call this thing, stablecoin or something else, if it has risks that are consistent with other products, we're going to regulate that like other products and that's what the guidance effectively says.

So in preliminary guidance the Swiss authority is looking at Facebook Libra, which again, well-publicized, would be based on a basket of underlying assets, fiat currency, some government instruments, details to be fleshed out, overseen by the Libra Association, details to be fleshed out, but

preliminarily the Swiss authorities said it would fall under their Financial Market Infrastructure Guidance, would require a payment instrument license under their regime, something a cross between payment instruments under the states and e-money under the EU Directive. They'd be subject to AML requirements, not inconsistent with probably what would happen in the United States.

But here's the interesting aspect. They then go that because Facebook Libra would likely increase the risk to the payment system, it should be subject to corresponding requirements to address those risks. What would those be? And again, the version I read was in English so I'm not sure 100 percent that the translation was great. But possible capital requirements to address credit, market, and operational risk, and matters to discuss risk concentration and the management of Libra Reserve.

A statement that the risk of the reserve must be borne by the Libra Association, not holders, but details to come upon filing a formal application. So the Swiss authorities in response to request for

specific guidance to specific items; payment license, AML requirements, the rest to come. It’s hard to develop a system with the rest to come.

Now, in my view, stablecoins have great potential to expand the usage of blockchain technology. We all know about the inherently slow processing speed of Bitcoin and some of the other cryptocurrencies. Vis-à-vis some of the existing electronic systems out there by private vendors.

But to Commissioner Berkovitz's point, if there was ability to have a comprehensive blockchain-based system, for swaps, and we know ISDA, by the way, is creating protocols to help potentially advance that, if there was a comprehensive mechanism to capture swaps online subsequent events to move payment instantaneously, that was valued instantaneously, very, very powerful because obviously if it's all happening on one system reporting is almost a weird concept because the information is there to see all the time through oracles or whatever that the government might utilize.

Stablecoins have the potential to help

transactions, internationally. But the regulatory environment today is unsteady, even if you get down to the different analysis, as I said, with the gold based on allocated gold - - a coin based on allocated gold is probably no different than a warehouse receipt and any kind of existing regulations that apply to transmission of warehouse receipts should apply. That's easy. But once you stop moving gold based on unallocated gold, that's an issue. Coin based on allocated or unallocated gold and something else, that's an issue. I mean, every permutation.

And by the way, this is just public blockchains. We know that there are initiatives by corporations to have privately developed things like stablecoins, the JPM coin, good example. On a private permission blockchain, not out there in the general public, should have entirely different issues.

In fact, the SEC recently issued a No Action Letter in connection with a chartered air company, TurnKey Jet, that wanted to have their own thing like a stablecoin, TKJ coin, and said not a security. But there were a whole host of things that the SEC said

were critical to that determination, not just the fact that it was a stablecoin backed by 100 percent of the relevant fiat currency totally - - only accessible only on a private blockchain effectively by the users of services to get chartered jets.

So we're a long way away from regulatory certainty, and I fear that there is a certain amount of turf fighting that's out there. You saw that in the reaction to the Facebook Libra project. Privacy concerns, banking concerns, central government concerns of what happens if it's widely accepted? Does it undercut the central banks? Significant issues. But, again, my point is a lot of these issues are simply amplifying difficulties in the law already existing in connection with existing financial instruments. The advent of crypto assets has simply amplified those difficulties and the introduction of stablecoins, again, just another step on the way.

Lee?

MR. SCHNEIDER: Thank you, Gary. If it would be helpful, we have in the slide deck a bunch of different examples of stablecoins, and I thought maybe

I'd walk through a couple of them just to be indicative. So if you look at slide 6, and we've got it up here on the screens, Tether is as Gary mentioned the fourth largest market cap, and by the way I'm just using market cap colloquially here, I don't mean market cap in terms of market capitalization of a stock. Market cap is a term that's been broadly adopted in this space, one that I find to be not accurate, but we'll use it for convenience purposes.

So, Tether was one of the original U.S. Dollar stablecoins. It goes by the symbol USDT. And it's designed to give people the ability to pay in U.S. Dollars, and then receive in exchange newly minted Tether stablecoins. And each Tether coin is supposed to be worth a dollar. The coin itself trades on third-party exchanges, and sometimes is actually worth slightly more than a dollar, sometimes it's worth actually slightly less than a dollar, but it generally stays within a pretty tight band around a one-for-one value with the dollar.

Earlier this year, the New York Attorney General initiated a suit against the makers of Tether, and

alleged a variety of potential violations under New York law. One of the key facts that people learned, I think, as a result of the Attorney General's action is that the company behind Tether was not actually holding one-for-one dollars against all of the outstanding stablecoins, but rather was using a combination of dollars and certain other assets, including debt instruments or loans with affiliates, to approximate that.

Now, as Tether pointed out in their court filings, they were keeping about 70 to 75 percent of the coins backed by U.S. Dollars, and they did a comparison of that to your typical bank account, your demand deposit account, where banks are not required to maintain anywhere near that level of backing for it.

So, Tether is one example. And, again, as Gary mentioned, you can see a situation where if all of the Tether coins are represented by underlying dollars, it looks very much like warehouse receipts or bailment type of activity. But what the analysis is in light of some of the facts that came out as a result of the

Attorney General investigation is still somewhat unclear.

And by the way, Tether claims they made all kinds of disclosures about the mix of assets that might be backing the coin, so I don't mean to suggest Tether is wrong and the Attorney General is right or vice versa, that's still to be decided.

The next one that I'll talk about is also on the same slide, TrueUSD. They have a bunch of different stablecoins for other fiat currencies. They are -- they represent to the world in their disclosures that it's 100 percent backed by the referent fiat currency. So that would be as distinct from the situation with regard to Tether. Gary mentioned the Turnkey jet situation. We have a short discussion about that, as well as Libra. Obviously Libra is still in the proposal stages. And so, we don't have clarity on exactly how it will work.

And what roles of participants will be with respect to Libra, but I would like to emphasize here that understanding the roles of the various different participants can also be very important so while the

"issuer" of the stablecoin might have one set of regulatory obligations, other participants who work with the issuer may have other regulatory obligations based on their activities. So for example, and this is not the case at least as Libra has so far been described, but if you had a stablecoin that was like a one of the SPDR ETFs, that was mimicking an index, you might have participants who are engaged in trading activities on behalf of the underlying pot of securities in order to maintain the balancing as against the referenced index.

And so, in those situations you would say, well, they are engaged in securities trading activities, maybe they need to be registered as broker-dealers. So, you need to not just look at what the issuer is doing, but also what other parties involved are doing.

The last one I wanted to reference briefly is the Paxos gold coin. That's on the next slide. Paxos Gold is designed to give a stable value as against gold. And the gold is actually in bars in Brinks' vaults, so we know there's custody of the gold. Now you can redeem your tokens if you're an individual

person, you can redeem your tokens for U.S. Dollar value or for some specific gold, physical gold, but institutional participants are also allowed to redeem for unallocated gold. And as Gary mentioned, there could be some differences in terms of what the legal treatment of this asset is based on what you can redeem it for.

Maybe let me just make one last point, and we'd love to answer questions that you all have. But the last point I wanted to make is the disclosures that are made in connection with the stablecoin are hugely important. I think the idea of good quality disclosures, so that people know what they are getting, so that people can evaluate what it is that they are purchasing, are the benchmark or cornerstone of regulation in the U.S., they are the benchmark and cornerstone in fraud cases. And so, focusing on the types of disclosures that are being made is, I think, hugely important.

MR. DeWAAL: And the last thing I'd just like to point out is not only are regulations obviously different, that's existing the case, so same things

can be regulated differently in different jurisdiction around the world. But from the perspective of an individual regulator in any one country, an instrument can be fundamentally different. A stablecoin based on USD, it maybe has one treatment in the USA but that same token sold to a citizen in a foreign country, a non-U.S. country, depending on how it is marketed it could be a straightforward speculative investment because obviously there is currency arbitrage immediately, if someone is paying Uganda currency against a U.S. Dollar coin immediately there's a speculative play. And someone could solely be buying it not for transactions, not for inherent value, but in fact as an arbitrage opportunity. And therefore, fairly a regulator could take a very different view as to what the nature of an instrument is simply by where it's sold and how it's marketed. And with that we're happy to take some questions.

CHAIRMAN GORELICK: Thank you. While everyone is thinking of their questions and putting their name cards on their side to be recognized, I'd like to start off with one question.

In very excellent lawyerly fashion, both of you said "maybe" a lot. You said "it depends" a lot, you said “it’s uncertain” a lot, and I think ironically said “unstable” on some occasions. Do you have any advice -- I’ll break this up in two parts, for the Commission and for policymakers about how to start to clear up some of this ambiguity?

And secondly, do you have that similar advice for industry participants who are struggling to figure these things out?

MR. DeWAAL: Particularly for this agency, you know, the only thing that is clear to me, and I didn't see Jamie Macdonald here, is that absent something, you know, clearly being a security if someone commits fraud in dealing with stablecoins, it is likely that the CFTC will have jurisdiction for antifraud under 6(c)(1), and to the extent there's leverage there could be obligations for folks to transact to a futures Commission merchant and/or on a licensed exchange.

I don't think the analysis for this agency is necessarily different than any other virtual currency

to the extent that's the nature of the stablecoin. It's get a little trickier where the stablecoin is really stabilized through algorithmic, and again there's a very, very important SEC case, there was a settlement last year, *EtherDelta*, against a proprietor, one of the original developers of *EtherDelta*, that effectively said if there's a requirement that something be traded on the exchange and the fact the exchange is algorithmic, someone's responsible and we're going to deal with that.

I know that Commissioner Quintenz right about the same time issued -- in a speech said something similarly that somebody has to be responsible if there's a violation. Those probably precepts still apply. But I don't see necessarily this Commission, you know, having the basis to expand the definition of a swap, for example, to capture, although the plain language arguably captures many stablecoins, but it would be an extension to believe that.

To me, the regulators internationally have to figure this out. Again, it's a bigger discussion, because the fact that you look, as Lee has said, as I

have said, at an instrument, we've been dealing with electronic manifestations of things for a long time. The only difference now, we're labeling them now stablecoins or labeling them virtual assets, okay? And that the technology is a little different, blockchain, Distributed Ledger Technology. But we've been using SWIFT, we've been using all sorts of electronic ways to settle transactions for quite some time now, and there's been law that's developed around that.

You know, as I said, I like what the Swiss regulators said. Same risks, same rules. Okay. But we shouldn't be looking -- and I hope the regulators are not looking to expand. It's confusing. And yes, if we can solve some of the confusion among similar type of products, that would be very, very helpful. Okay? But to the international organizations, whether it's IOSCO, these discussions are important to have, and it's important to have some kind of, you know, consolidation. But probably at this point that's best to get it.

I mean, the FCA earlier this year issued guidance

on what it thinks is within its perimeter, regulatory perimeter, those kind of thinkings are good. Issuing guidance is good. Issuing the views of regulators is good. But at the end of the day people come to us, outside counsel, and they to ask our views and we really have to break it down and we have to talk to the regulators, and we try to get the answers from the regulators the best we can. There are very few formal opinion letters issued these days in this area. You get some reason views and you hope you can go forward, but as we saw with Basis and SEC, sometimes you end up hitting a road block and pull back and you've lost a lot of money and that's not very productive.

MR. SCHNEIDER: Let me just add to what Gary said.

Most of my maybes and uncertainties were around trying to develop a category called stablecoins. I actually think that most of the time, if you look at the functions and features of a particular token or stablecoin, you can come to a conclusion as to what type of instrument it is.

So, my purpose hopefully is not misconveyed. I

don't think this is some new wacky, weird world that needs to be discovered. Rather, I think we need to go back to existing principles, go back and look at existing types of instruments, and do what lawyers and regulators have done forever, which is this looks exactly like that, and so we're going to treat it like that. Something else looks like something else, we're going to treat it like the other thing that it looks like and not try to reach out and create new categories that are just dependent on the fact that there's encryption technology and blockchain technology involved here, as opposed to some other kind of database technology.

CHAIRMAN GORELICK: Thank you. Superna?

MS. VEDBRAT: So this is very informative. I actually have two questions. One, if you could just, you know, give us some examples of what are the attributes or characteristics that stablecoin brings, advantageous ones, relevant to whatever reference asset it is linked to.

And then the other is, is there any similarity in stablecoin and, you know, the exchange of value that

you see in applications like Venmo?

MR. SCHNEIDER: So to answer your second question, look, I think that stablecoins can be an important payment rail. I have some skepticism whether stablecoins in a country like the U.S. are necessary given the way the dollar functions and the existing payment rails we have, particularly now that the Fed has announced they are going to go to 24/7/365, Fedwire and all of that.

That said, there are obviously other countries in the world that could benefit from stablecoins, and to the extent that people in those countries want or need access to a U.S. Dollar based-type of stablecoin that could be hugely useful for them. Now remember there are other types of stablecoins not designed to be currencies, one might say although the Paxos Gold stablecoin is a stablecoin, referent asset, gold, tends to be volatile at different times in the investment cycle. You might say that’s not particularly stable and wouldn't want to use that as a payment tool. You might want to use that as more of an investment tool.

And the same would hold true for any other type of stablecoin that you could dream up. For example, I talked earlier about an ETF like a SPDR-ETF where it's an S&P 500 Index or some other S&P Index-based coin. Again, that would be stable against that referent index, but to the extent there was volatility of that index probably not particularly stable and not maybe that useful as a payment mechanism.

Gary, did you want to answer her first question?

MR. DeWAAL: Yeah, I think the attribute is tied to what I said before. To me, the power of the blockchain is the fact that it brings to one relatively transparent location, a lot of transactions and a lot of information and things can happen in a relatively efficient way. Whether we're at that point, whether the answer is a private blockchain or public blockchain, those are things we can all debate. But to me, the power of the blockchain is dealing with what Commissioner Berkovitz has sort of said, something he sees from a regulator point of view, which is bringing things to one location.

And to the extent that, you know, there are

international aspects of transactions, the extent there are transactions outside the United States, then to the extent that the settlement can occur, so that if I move a JPM coin, I know even no matter what time of day I get it, I have immediate ability to translate into whatever currency I want, that's powerful. And again, coupled with a complete system, this is all powerful stuff. This is nirvana view. And we're probably not there yet. Okay? But we will get there. Okay? We will get there.

And my guess is it's only a short matter of time, Christine Lagarde said it's time for the Central Banks to be exploring the issuance of their own digital coins. And I think that we will see the combination of blockchain technology and some kind of another form of electronic currency really being very helpful tools going forward.

MR. SCHNEIDER: Just to add one quick point to what Gary said referencing the infrastructure comments from Commissioner Berkovitz and also Commissioner Quintenz's comments about using blockchain as a possible way to help with compliance infrastructure,

there is, in my view, a very good paper that just came out of the Bank of International Settlements about embedded supervision and how regulators and financial services industry supervisors can use blockchain and its capabilities to better further their mission in a much more effective and efficient fashion. I highly recommend it to anybody who is interested in that topic.

CHAIRMAN GORELICK: Thank you. I think we have time for one last question. Yesha, I saw your card up.

MS. YADAV: Great. Thank you for this very informative and insightful presentation. I just had two questions.

The first references Chris Brummer’s testimony in relation to Facebook Libra in an issue that came up there. Some of the sort of potential reference assets, for example, the British Pound or the Yuan, gold as you said just now are - - have been extremely volatile over the last year. So we've seen rapid devaluations in response to market events. And in that context how do you envision issuers of

stablecoins having and developing the expertise in valuation, in sort of developing the ability to deal with adjustments, rapid adjustments to make up for shortfalls, that would happen in this context?

And the second question is in relation to stablecoins that are pegged to dollars. In that context, how would users or retail users, for example, distinguish such stable coins from digital representations of value in their online bank account and in that context when that is the case, how effective is disclosure as a protective mechanism when we're dealing with retail users that may be prone to panic, that may sort of want quick liquidity for their assets, and how will disclosure help them in that case?

MR. SCHNEIDER: So I seem to be answering second questions first for which I apologize, but I do think the second question is a very good one. And my belief is that just as researchers and others have adopted ways to value what we consider sort of traditional financial assets, the same will happen with regard to stablecoins. And that's why from my perspective an

emphasis on disclosure is important. Because in order for -- and, look, it's the same emphasis on disclosure that’s already embedded in the Securities laws and the Commodity Futures swaps laws, you have to understand what the thing is and once you understand what the thing is, then you can figure out how to use it, how to value it, and how to regulate it.

And to my mind, that's where you focus on the functions and features and the disclosures so that people can develop models that will be useful for them.

MR. DeWAAL: I guess I get the first question, again. I don't see managing a basket of assets to Libra any differently than managing a basket of anything where you're trying to achieve a result. Obviously people will develop expertise, trading expertise, they will figure it out over time. My guess is obviously they’ll be using mathematical models or computer models and there will be algorithms. And that’s why there are already algorithmic stablecoins that achieve the stability of price through algorithmic mechanisms to basically sell

a little of this, buy a little of that. You know, whether they are underlying cryptos or something else, there are mechanisms that people are already developing. That, too, goes to disclosure.

Folks need to understand how that works. And you know, there's no guarantees of anything. That should be made clear. But, again, it is the nature of that ability to change baskets, that I think is what will get regulators' eyes. The more that it sounds like it's basket picking, the more it's likely to fall into somebody's regulatory oversight, collective investment vehicle, you know, depending on underlying issue, it could even be a commodity pool, who knows. It depends what the underlying instrument is.

CHAIRMAN GORELICK: Okay, thank you, Gary. Thank you, Lee. At this point I think we are ready to hear from Chris Brummer, Professor and Director of the Institute of International Economic Law at Georgetown, and Tom Chippas, the CEO of ErisX.

Chris and Tom will present on the issue of crypto asset custody. Thank you very much.

MR. BRUMMER: Thank you so much. Great. Thank

you so much for having us here today. It's a real pleasure to be here with you and I applaud Commissioner Quintenz's leadership in helping to direct the attention of the agency to many of these cutting edge issues. Indeed these are cutting edge issues. And as I tell my students, expertise is relative as opposed to absolute. And as a result, many of the comments that I'll be making today are intended to provide an overview of some of the relevant comments, and then as I present and sort of walk through some slides that I've presented, Tom is going to be able to chip in as well and provide his expertise and view and to help extend the analysis provided in this larger, again, overview of custody challenges in the digital asset space.

Okay. So I guess our first slide goes to this question, and I think it really fits in very well with the previous panel. Ultimately, when we discuss the question of custody, custody is a critical aspect of market infrastructures and market activities more generally. Indeed holders of digital assets without some kind of custody tools don't have the means of

making a market and as a result, custody is a question that really goes to a foundational matter of market making and goes to one of the core building blocks of building any digital market infrastructure.

But custodying digital assets and cryptocurrencies is not easy. And cryptocurrencies, as we all know, are essentially digital bearer instruments. I'd like to suggest in the context of custody, this is important and it's more than just a matter of asking whether or not cryptocurrencies fit into sort of pre-established frameworks or guidelines. I mean, when you think about what this means, it creates unique challenges from both cybersecurity and governance perspectives. So from a regulatory perspective you have to think what those differences are and then obviously try to map out an appropriate industry and governmental response.

Custodying crypto assets also is at least right now characterized by a varying array of different kinds of coping techniques. And these kinds of coping techniques as I'll get into shortly, deal with an array of different kinds of uncertainties that

permeate the market. But from an infrastructural perspective, the very concept of custody itself has to be inspected a little bit closely because it can infer or indicate responses that could include a transactional custody approach, where an institution or entity is custodying a digital asset or cryptocurrency for a discrete transaction or purpose versus other kinds of custody infrastructures that are intended for more indefinite and prolonged relationships.

Let’s move to the next slide.

It's also important to highlight the fact that custodial relationships vary. Now, there are lots of different kinds of terms, usually terms of art, used to demarcate what those relationships are, but I think that the world can ultimately be divided into three basic custodial relationships. There are the noncustodial wallets that certainly I prefer and I think others prefer, the word self-custody, because it's a more concrete indication as to what is expected of the person who is indulging or using or employing this particular custodial solution. And then there

are the exchange-based custodial wallets. And then finally, there are the third-party custodians, so the non-self-custody, the non-exchange-based custodial wallets.

One of the themes that I'd like to share with the TAC today is that when you think through custody, I'm the bearer of bad tidings, that there is no magic solution, really, as to trying to navigate the world of tradeoffs that ultimately come across different custodial solutions. That is every custodial we will discuss holds and has certain kinds of disadvantages, and as a result there will have to be some kinds of policy decisions and also market-based decisions as to what is most appropriate given the infrastructure being deployed and the kinds of customers that are interfacing with that particular custodial solution.

Now self-custody is one where from a disadvantaged sort of perspective, customers are ultimately the weakest link in their own cybersecurity. And this raises particular red flags or at least concerns where retail investors and rather unsophisticated users of digital assets are employing

this particular custodial solution. However, the self-custody solution does offer unexpected advantages in so far as it helps to enable decentralized architecture that creates lower pay days for cybercriminals. As a result, they can represent harder targets, especially when significant resources have to be deployed in order to infiltrate any particular wallet.

Again, getting back to the disadvantage, self-custody solutions are not always interoperable with either exchange-base the solutions, which we'll get into shortly, or even the sort of third-party custodial solutions.

Now exchange-based wallets, certainly the kinds of wallets many of you are focused on and thinking through, ostensibly help to cure many of the shortcomings of self-custody. Now the advantages for customers are readily apparent. They are usually rather easy to use, they can also provide a kind of one-stop shopping venue particularly with exchange platform providing a variety of services. They can also offer greater cybersecurity and sophisticate than

at-least most retail customers.

The challenges accompanying any kind of exchange-based wallet is almost an irony of being successful is they can grow large and that they become the proverbial honey pot that we've seen in the past, where they become a target for cybercriminals. That ease of use and the one-stop shopping function also carries the disadvantage that you have collapsed financial functions that arise in any particular entity. So where you can have an exchange ultimately engaged in not just a custodial function but also market-making and the provision of a trading venue.

Now, this in itself creates many of the kinds of risks and concerns that the Commission has always had its eye out for, including the comingling of customer assets, you could have different varieties of front-running, market manipulation, these kinds of problems can be particularly high-risk, especially in the absence of supervision and regulation.

And then finally we have as I mentioned a final option, which is the concept and possibility of third-party, non-exchange custodial solutions. And now

these can offer greater cybersecurity and sophistication than a traditional retail holder would enjoy certainly under self-custody. And they may alleviate, but not reduce or eliminate, the risk of exchange-based wallets where custodians are separately regulated, affiliated entities. It's important to also note some of these non-exchange custodial solutions can also be important where an institutional investor could be looking to have access from -- looking to have multiple individuals access certain kinds of assets, and customers may require certain more bespoke access controls and permission settings.

MR. CHIPPAS: Just to comment now that we've talked about both the exchange and third-party options, hearkening back to the previous slide briefly, some of the issues that Chris points out with respect to comingling of assets, front-running, market manipulation, et cetera, many of these concerns were raised in a report last year published by the New York Attorney General regarding virtual currency markets, and there is a whole parade of horrible things that most financial markets, professionals, would be aghast

to have seen. And I think it brought to bear -- to the fore I should say, that these potential conflicts of interest can exist when you have deep vertical integration in some of the existing spot exchanges but stepping back for a moment and considering the core principles any operator of a DCM or DCO needs to abide by, many of these issues wouldn't exist or go away or be expressly illegal.

So although not directly a custody point, I think what we're trying to highlight here is that the custody choices made to-date in certain spot markets may make the risk of some of these things higher and the regulatory regime in which they operate under a little less clear. Whereby, today under the CEA or even under 1940 SEC regime, some of these issues don't exist or would be expressly wrong.

I think that third-party custody doesn't per se solve all of those but disaggregation of some of these components remove some of the temptation that might not otherwise exist.

MR. BRUMMER: Right, and even those as we note are not, again, perfect solutions, and they do carry

some disadvantages at the same time, but it will be interesting and I think one of the challenges of the Commission will be to see exactly how that market segment ultimately evolves. And there would be to the extent to which there's greater proliferation in particular of the third-party non-exchange custodians, greater monitoring challenges given potentially larger number of services providers.

We are all very familiar with the basic custodial infrastructure and I'll go quickly. Although, I did want to just highlight something briefly.

Obviously, the world can be sort of divided into the hot wallet versus cold wallet world of custodial services. It's just useful to keep in mind that each of those solutions, again, involve a kind of tradeoff. And one way of looking at the tradeoff, is whether or not to the degree to which there's a tradeoff of liquidity and ease liquidity management vis-à-vis increased cybersecurity risk.

And also, there's this question of scalability and the question of how costly is scalability with either one of those two solutions, so when you have a

kind of digital markets infrastructure and electronics infrastructure, it's easier to scale. Whereas, with the cold wallet you're off line, you're trading at-least safety, although again there's still some human risk where you have individuals physically pulling keys out of storage. You're trading that safety for more illiquidity in terms of speed with which transaction can be executed, where there is a greater reliance on cold wallet.

And there are questions of a more challenged nature of scalability and when you get into that scalability question, then you also have accompanying cost questions. In fact, we were just sort of sitting around drawing -- literally triangles of potential trilemma, for economists around the table, as perhaps there is one existing between cost, scalability, and --

MR. CHIPPAS: Liquidity.

MR. BRUMMER: I'm sorry -- cost, security and liquidity, and to what degree are ultimately custodial solutions able to achieve two of the goals but not necessarily all three.

MR. CHIPPAS: I would add that it's cliché but true, technology is an ever-changing thing. If you were look at the custody of digital assets several years ago, commercial providers would have espoused about their bunker deep in the mountain guarded by burly people with weapons and controlling access to USB drives and things like this.

We've moved on from there to a combination of taking devices, storing private keys offline, and putting them into secure locations and putting in place robust operational flows in order to utilize them when necessary, but looking much more like a bearer instrument and how one might secure a bearer instrument. And the debate is already moving to new technologies -- well, newly applied, not new technologies, like multi-part computation, and the Commission may find itself one day having to consider whether or not custody is simply the assumption of liability because the technology is widely available, and perhaps made available by pure technology companies, as opposed to what brand of computer does my custodian use today to keep track of its books and

records. And that is an inflection point that is not here yet, but it's actually not that far away. So this space is evolving rapidly and I think to previous comments made both by some of the Commissioners and by previous panel about the application of principles, it would be very important for the Commission to maintain focus on principles here because it would be virtually impossible to stay up with the changes in technology and then evolving operating models thereof, specific to digital asset custody.

MR. BRUMMER: And just to highlight that, obviously there’s as technology evolves, you're dealing with different kinds of solutions where you not only having innovation on the digital infrastructure-end, but also on the technical exclusions, you're dealing with the procedural-end.

MR. CHIPPAS: For sure. And potentially, commercial model as well.

MR. BRUMMER: And the commercial model as well. That really does make this very much a moving target.

What also makes this challenging and difficult,

is that we've been talking about retail investors or holders of crypto assets, but we're also obviously in an increasingly professionalized ecosystem and you see that there are lots of different kinds of custodial players as well left off that list, but one of which is enormous interest to you all would be clearinghouses as well, but you also have the banks, trust companies, broker-dealers, and others.

And therefore, particularly in a world as we heard in the last panel of a kind of transitive theory of legal asset identity where one kind of -- you need a Ph.D. in physics to understand sort of the transition of one digital asset and the transformation of one digital asset from a security into a commodity or the like. You know, you also have to think about repercussions throughout the ecosystem like what are the consequences for how you not only oversee but supervise custodial players when the digital assets themselves may move or evolve in terms of their legal classification and identity.

Now one of the observations that we had made in conversation with members of the subcommittee was just

that you have at times an assumption, when you think about how markets evolve, and when you think about the question of the institutionalization of markets, that there's always the kind of competitive advantage that some of the larger incumbents in closely related industries may have, vis-à-vis the smaller players, but this market is interesting because many, at-least with the headline-grabbing entities in the digital asset space, tend to be sort of less incumbent, more of an upstart innovative FinTech firms at raising certain kinds of questions about the ultimate involvement and the timing of involvement of institutional players, and there is considerable skepticism or at least concern in the institutional market as to the degree to which they should be involving themselves in this digital asset custody space.

And there are some causes or drivers that one can identify. There's inherent riskiness of the asset. Again, dealing with everything from cybersecurity to technological questions, to the legal questions. There's a lack of familiarity with digital assets even

vis-à-vis some of the upstarts, who maybe started at T1 with a deep and abiding interest in the underlying technology.

There's still also the questionable robustness, two different kinds of cybersecurity and technological and operational risks. And then, there's clearly the regulatory compliance and litigation risk, when you're a larger player and you have resources, you know, what happens in the wake of any kind of malware attack or hack.

MR. CHIPPAS: I would add and this is a personal view, not a view of the committee per se, that most of the institutional custody players today are sort of lagging in their knowledge of this. They have innovation teams, people that look at technology, but if they were to enter the marketplace today and attempt to provide providers of custody services, they'd find capacity outstrips the demand today and there would be a robust number of technology providers or service providers that could work with them to enable services as they so chose.

It's this last point that Chris mentions, I

think, around regulatory compliance, litigation, and risk that gives a lot of the natural pauses in those larger organizations where digital assets are relatively small compared to other businesses they engage in today, but the risk is outsized as compared to risk in the other asset businesses they engage in today.

That is my personal opinion but I do think it's something with minimal amounts of inquiry you would find likely to be true.

MR. BRUMMER: Those kinds of questions are obviously -- well, I think my slide --

Now, getting to the question of the litigation risk and regulatory compliance questions, again, I don't want to differ with the ultimate conclusion of previous panel in terms of saying, look you have to go and you have to think through how different really are these digital assets vis-à-vis what we've had in terms of legacy financial products and instruments, but there are differences and some of these differences in terms of the infrastructure and the technology and the governance mechanisms enabled and executed through

that technology raise a number of questions, especially against the back drop of our traditional expectations that seem to -- of custodians, that seem to be present across different regulatory spheres.

No matter whether or not you're dealing in SEC-land or CFTC-land, there's a general expectation that a custodian maintains physical protection or control of customer assets, you see always the kind of proficient against comingling of assets, particularly customer assets and that of the firm. And then, I have in sort of parentheses, I think that there's clearly an expectation that there's delivery of customer assets to the customer in a timely manner and/or when contractually agreed upon.

Now those kinds of expectations are challenged or at-least made more difficult in the context of digital asset forking. When custodians are in possession of cryptocurrencies when a fork arises, you have a number of important questions that arise. Is the custodian required to return to the account holder the forked cryptocurrency along with the original cryptocurrency?

Importantly, what is the speed with which new

forked cryptocurrencies must be delivered to the account holder? What are the technical limitations and the cost of delivery of the new tokens to the custodians? And then, what disclosures, and we'll get to this a little bit later, should be required for customers regarding forking policy?

MR. CHIPPAS: Yeah. It's another scenario whereby anticipation of possible outcomes is impossible. What if a commonly accepted token was forked into a stablecoin of currencies of countries on Treasury’s OFAC banned lists or what have you. The custodian might face some serious issues with trying to maintain that.

So to-date what you see typically is disclosure of a forking policy, and most involve some aspect of timing notice whereby holders of the actual assets are able to remove them from custody, which is a burden in terms of their usability and perhaps third-party costs, as well, in order to receive those forked assets and then they have to return them back in. So it's certainly imperfect today but similar to previous panel, disclosure is key in these regards so that at

least consumers of the custody services can determine whether or not the forking policy is appropriate for assets they intend to hold.

MR. BRUMMER: Another question that arises especially when you start to think about the international dimension of many -- of the trading environment for many digital assets, but even here domestically it’s something that could be termed intercustodial relationships.

Due to the cybersecurity questions, as in the context of a hack or volume or because of demands for withdrawals, exchanges, registered and unregistered, can face liquidity crunches. Particularly when you're operating in an environment of a very thin market for a digital asset. And the inability to redeem customer -- against a back drop of customer requests, can harm the reputation of a custodian and as I’ve heard more than once the faith in the industry. So it's like going to an ATM and unable to withdraw cash, and asking yourself, okay, do I trust ATMs across the country?

Custodians as a result may lend digital assets to

one another without full disclosure of such activities to their customers. And, you know, this raises a lot of questions. It doesn't necessarily mean they are going to lend or provide funding resources using customer funds, although we've seen that stranger things have happened.

Instead, it could mean that some of their other resources used to bootstrap or to provide a cushion for their own activities may find themselves sort of lent out in different ways to help stabilize markets, but it could ultimately end up creating questions about the security of those customer assets.

So we end up -- and I think -- I took Yesha's question to heart, about my Libra testimony over at the House earlier in the summer. We, too, end up with this question of disclosure, which is that given the fact that there are no silver bullets and given the fact there are tradeoffs, no matter what solution one is engaged in. Some kind of disclosure regime in plain English, is and would be necessary even for the general health of the industry, and we think that that disclosure should entail really a disclosure of the

full spectrum of potential counterparty risk from cyber security practices and limitations, operational risks, the conflicts of interests depending on the business model of a particular entity, perhaps information on balance sheet or capitalization. Certainly information in terms of the forking practices, so that a customer is aware of how the exchange or the custodian will respond when a fork arises.

And then finally, this question of whether or not the digital asset custodian is ensuring those digital assets or whether or not a customer is expected to go out and engage in self-help and to find some kind of insurance herself, and to provide some indication as to whether or not that insurance is only for those assets held in a hot wallet or whether or not it's only for those digital assets held in storage.

I did want to add just two quick points. The cyber security and practices, you know, of all those perhaps that's the most tricky, right? Because if you disclose too much you're providing a road map perhaps to a wrong-doer, and so you'd have to think that

through thoughtfully.

And then secondly, getting to the question on the previous panel, you know, is or would this kind of disclosure stymie or prevent some kind of run in the case of a hack, which I think is an excellent question. And my sort of thinking here is, well, I'm not certain that it would necessarily stymie or prevent a run but I do think that it is important, especially in a world where you see more retail investors or holders of crypto assets in this space, that people know not only what they are buying but who is holding it. And what are the attendant general risks that accompany that choice as to where and how they are ultimately storing their crypto assets. And it will be a delight and an interest in watching how the Commission tries to integrate and to adapt by thinking through certain kinds of disclosure issues that have been traditionally, perhaps the province across town, but as these issues fall into your lap, I think that they will be more important.

CHAIRMAN GORELICK: Well, thank you very much, Chris and Tom. That was a very informative

presentation. I would like to open up the floor for questions and discussion about this presentation.

Yesha.

MS. YADAV: I feel terrible for asking another question.

CHAIRMAN GORELICK: You're good about it.

MS. YADAV: I feel bad. But I'm delighted to see that Tom and Chris have Law Review article in the making, as well, which is very exciting.

So I guess my question is having outlined a really fascinating -- through a really fascinating presentation, this array of risks and costs that custodians are facing. In addition, obviously the forking risk you raised.

You know, I guess the inquiry that I have is which credible players would really want to do this? This really seems to entail a great deal of resource management, enormous amount of logistical warehousing, support, constant vigilance on the part of providers. Why would providers want to get into this game, credible providers, resource providers, want to get into this game?

And related to the extent they do and want to pass on their costs to retail customers, are we creating the danger that retail customers then back away from this custodial system and essentially become the self-custodians that Chris was talking about with the sort of diminishing impact on liquidity and the use value of these assets overall. So that's really the concern I had here.

MR. CHIPPAS: Well, maybe continuing like the previous panel by answering the second question first. With respect to retail today, I think you would find that most crypto-natives are big fans of phrase, “not your keys, not your coin.” So today there's a substantial number of retail participants that engage in self-custody. What will be intriguing to watch as marketplaces evolve, as new people enter the digital asset space, is their concern the same? Do they have the same ethos? Do they also want to engage in self-custody. People don’t self-custody their equities, for example, today, they just assume the books and records at DTCC are accurate.

So to that end, the second question is moving in

the opposite direction. So I don't think there's a concern I would see initially.

With respect to the first question, I'll reference my comments made during the presentation, that there's solutions today. It's a competitive marketplace for high quality solutions offered by a multitude of providers, it's already moving onto generation two, and three, and beyond.

So in all sort of technology-driven businesses one would expect cost to go down, not up, and the entrance of new competitors should keep that natural economic check on potential growth. I think that the reason when we say top tier and think about folks that are engaged today in custody of equities and other assets, the cryptomarket is just very small for them right now, so the comment I made about risk and reward tradeoff is probably the primary motivator today for why you don't see them running into it.

MR. BRUMMER: Yeah, and I'll just add, I think that when the market becomes more speculative, right, I think it's a safe hunch that when you see a ballooning or big jumps in terms of the valuation of

digital assets, that that tends to lure in individuals who may be less sophisticated and as a result you can see more of an inclination to engage in or to rely on exchange-based or third party custody solutions as opposed to sort of your first movers who may come to the market, as former engineers with more sophistication.

I think that the technology in this is absolutely right. I want to again emphasize that this cost question is going to rely in both the procedures being deployed, as well as the basic choices, as to whether or not you want to have a hot or cold wallet. And the way you scale with either one of those solutions will be different, I would suspect, right? If you have a cold wallet solution where there's more human interaction, where the physical person is engaged in pulling out private keys, then whatever scaling model is going to look perhaps more like a Ford assembly line kind of scaling versus what kind of scaling you would have if you're dependent on a digital hot wallet approach where you can literally build out volume based on a platform, and both of those would entail

different kinds of cost dynamics.

MR. CHIPPAS: That's what the next generation in technology is trying to address, is that scalability problem.

MR. BRUMMER: That's right.

CHAIRMAN GORELICK: Thank you guys. I think Larry had the next question.

MR. TABB: Thanks. One of the primary business models around custody is around lending and margin. And when you start getting into digital assets and issues, then with air drops and forks and complexities, how do you see that developing, is that something the Commission should be thinking about?

MR. CHIPPAS: I think the market's already addressed it. If you look at lending agreements in place today, they all have some sort of language related to forking. It's been thought about. And similar to the comments around disclosure, it's understanding what the lender expects and what terms the borrower and lender will agree to. So I think the market is finding it’s level, at least for the participants today. Perhaps the thing to think about

is if the range of borrowers expands from the folks that are in it today, they may demand new terms but as far as currently those sorts of questions are typically addressed in the lending agreement.

CHAIRMAN GORELICK: Thanks. Tim, I think you had the next question.

MR. McHENRY: Thanks, Richard. Thanks again for a great presentation. Are any of these custodial models particularly in the third-party custodian, are they giving thought to how to best demonstrate individual ownership to third parties like regulators, auditors that come in, they are all looking for a way to verify ownership so are any of these helping in that cause?

MR. CHIPPAS: So, short version, yes. There isn’t a uniform way, there's certainly some more focused on the pure cryptographic means, others on other forms of evidence, but in short, yes. And it's a actually point of differentiation for some custodians, really targeted at their end audience. So if you are looking for a custodian, say, because you want them to house a fund and you want to be able to

demonstrate as part of your NAV calculation, as ongoing proof, et cetera, there's some solutions oriented towards that. Others are more point in time risk-based, wanting to see what are the balances expected to see, “Can you show me that they are there?” So, short answer is yes. Long answer is there isn't one acceptable way to do it today. It's really dependent upon who the custodian is trying to service.

CHAIRMAN GORELICK: Chris?

MR. HEHMEYER: Thank you, Richard. Chris Hehmeyer. I have a proprietary and a cryptomarket making firm in Chicago and I wanted to offer a couple real life examples and then follow it up with a question.

One thing that in the previous panel that Gary talked about is how powerful some of these stablecoins are. And we went to -- we have a counterparty in Japan that we make markets, spot markets to, and Bitcoin. And I was going to visit them. We went and sat down for lunch with our clearing bank that's been our bank for 20 years. A well-known Chicago bank.

They do a great job, great people.

And we sat down with them about how long it would take to settle with a counterparty in Japan and in dollars, and they said, well, if it's in by 4:00 we can assure it guess done by the next day in dollars. If it’s in Japanese Yen, if they have a correspondent relationship with a correspondent bank that we have, we might be able to get it done by Tuesday, if not it will be Wednesday.

And so, I told that to our counterparty in Japan, and he said, “Forget all that, we'll settle in Tether. It will take minutes and there’ll be no charge.” And we were settling on a wallet-to wallet basis, settling on Bitcoin and Tether. And so, people are certainly using wallet-to-wallet and self-custody. We're of the opinion, of personal opinion, that the exchanges have done a tremendous job of bringing in retail accounts and principle-based trading firms in many way, and some of the early participants. And that in many ways, I believe it's because it's been their own money.

With institutions coming in with a board of

directors and the CFO for a larger institution, a company that’s contemplating accepting a digital currency, they want a very safe place for that money, that value, that will be then be in the position of United Airlines, not to pick on anybody, but if they are going to accept a digital currency or a digital token from the public that has to go someplace and these custodians have built tremendous systems for being able to accommodate that. And of course, there's five or six big brand names that are now coming into that space to provide that.

So we're of the belief that these custodians and some of the exchanges are going to facilitate the ability for these larger companies to accept digital currencies or tokens or whatever the token is, but typically digital currency and facilitate getting the digital token back into dollars so they can make payroll and pay taxes.

We make a market in those products and spot, and on -- I think we're on six different custodians, and it depends on the counterparty as to where they want to settle, we'll try to settle where they want to

settle the transaction.

We're on, I don't know, something like 15 or 17 different exchanges. And so, the liquidity is -- of course, these are relatively small assets in terms of market cap, but the liquidity providers are being aggressive and offering liquidity, and so my question is in the presentation there's a discussion about lack of liquidity and we go to these various firms and offer to make markets to give them a price and our competitors, Richard’s company is one of them, and they are very good at it. There seems to be a lot of liquidity being offered to people.

So how do you come to the fear of lack of liquidity on the -- as the custodians come to market?

MR. BRUMMER: So, one of our slides, and I assume you're referring to our slide on the cold wallet solution slide. Yeah. Our conversations largely focused on this question of, okay, if you're offline how do you literally access private keys quickly and particularly in a world where, you know, you're thinking and envisioning a world of smaller retail accounts as opposed to larger institutional players

who may be able to -- for which, I guess, accessing any particular set of private keys would immediately provide access to, say, a large volume of any particular digital asset, right? In which that in and of itself would provide significant -- is a liquidity move with very different qualitative features as compared to, you know, smaller retail accounts.

And so, the challenge is that when you get retail folks in the space of a cold wallet, you have to, even if I'm only holding $20 U.S. -- $20 worth of Bitcoin, if you have lots of different account holders and for each of those you have to go and access those private keys, right?

That's very difficult to scale, as compared to a more institutionalized environment where, yeah, you have maybe, you know, a couple players but they are trying to move such a large amount of funds that, again, you know, that raises entirely different and perhaps from a pure liquidity standpoint of trading less problematic questions as a world sort of dominated by smaller retail players, and that's the tradeoff we're trying to identify.

MR. HEHMEYER: Got it, thank you.

MR. CHIPPAS: Just to add to that Chris, it's an interoperability question. So the market structures that I see people trying to optimize, if I close my eyes and just listen, sounds like old FX, OTC market structures. And we've seen the negative consequences of that as FX prime brokers were created, they were the next great opportunity for them, they provided credit and liquidity and solved all that problem in the FX space, but everyone is exiting that business because no one wants to pay for it, there's large losses, and the participants rage against the ability for those FXPBs to control risk. You know, this isn't how it's done. Well, actually this is how we control risk.

So I think that that's probably a larger conversation but in short, there isn't interoperability today so the liquidity may be available, it just might be at the wrong place, at the wrong time. And that is really the gist of what we're trying to say, that it's not as free flowing as say the Japanese equity across TSE, Chi-X Japan, et cetera

where you don't ask where do I have the liquidity. It's just available in the market.

CHAIRMAN GORELICK: Well, thank you everybody for your questions. We are out of time for this panel. I apologize for any additional questions, we'd be happy to take up in the subcommittee.

With that I'd like to suggest we take a five-minute break and we'll try and get back on schedule. We'll hear from the DLT and Market Infrastructure Subcommittee when we get back.

Thanks, everybody.

(Recess.)

CHAIRMAN GORELICK: Thank you everybody. Now let's turn to our second panel, which will include a presentation from the DLT and Market Infrastructure Subcommittee. Our subcommittee members are Brad Levy, the CEO of MarkitSERV. Shawnna Hoffman from IBM Global Cognitive Legal Leader, that's a mouthful. And Yesha Yadav, Professor of Law at Vanderbilt Law School.

They will be presenting on data privacy and application of DLT in derivatives markets for custody

and collateral management. With that I will turn it over to Brad.

MR. LEVY: Thank you very much, Rich and to our sponsor, Commissioner Quintenz who is not here at the moment, but thank you to him for sure. And Shawnna Hoffman, my subcommittee co-chair and my co-panelist Yesha, as well. To Jorge our former whipper and Philip our new whipper, and Meghan for getting it all together, and obviously Rich, our chair, and the full committee. It takes a village and this is always an interesting journey with a massive tech space and to make it relative and interesting.

So I'm just going wind back to give perspective of where we've been. It's hard to define, so maybe a little bit of history might help.

So October last year we talked about this as a very big idea, this distributed ledger technology space. At the time people referred to it a bit as Internet 2.0, this massive new model of trust related to IoT. We talked about the broad issues in the space around operations, technology, regulatory and legal. And then the very broad applicability, whether it's

across asset classes, roles or functions, and we zeroed in on FCM function then.

In March, we came at a little bit more of a check-in on the hype cycle, which was fast and furious post the December run up and rundown. Across-industry adoption, we kind of set the timeframe as 2025 as maybe when things become truly impactful, changing everything. And we seem to maybe be close to halfway through that journey, which we all kind of peg as three, four, five years ago.

And then the applications, we focused around smart contracting, trade reporting, and recordkeeping, it’s come up quite a bit today. And then, we dwelled a little bit on payments. We talk stablecoins, fiat money in digital forms, and then more private networks that could leverage something digital.

So today we are going to continue in taking that wider tech frame to try to define what we're trying to talk about today and discuss and inform. Why? Because it's our mandate, so we're going to be very focused on tech. We will then take a pivot through a theme of privacy, which is very topical on the planet, and

Yesha will pick up there with an outcome of confidentiality, and then we'll dwell a little bit on specific technology around encryption, which is a tool that's very active in this space and again, has come up quite a bit. And Shawnna will pick up there.

More importantly, we'll pivot to market applications, really hanging around custody for a bit and I think it will be an interesting interplay between our conversation and the previous with Chris. And then, speak to some others as well which seem to hang a little off of privacy or a bit more identity-centric and wander through some use cases.

So a little less legal chatter by design, but I'm sure we'll speak to it a little bit here and there because it matters. It won't be highly technical hopefully, but it will certainly involve tech, and I think per our Chairman, we'll achieve that perfect balance of speaking in a high level way, technology-wise, and hopefully bringing ourselves down to earth to speak about practical things.

So I will kick off with this larger tech framing and this has come up a lot today, many straight men

for this panel of men and women, I have the women on my panel which is great, only straight men so far, but there's a clear thing going on where this world of crypto, or virtual and physical and more tangible is not distinct or disconnected. A lot of the concepts are playing between the two worlds, we're all going to benefit from it all, from a technology perspective.

So when you think -- and there's applications proliferating everywhere, whether they're all doing big things or not is a different question but private equity use cases, equity stock, repo, traditional markets. Again, a lot of the same issues coming up there that you'd see in the crypto or virtual space. Reporting, settlements and payments and obviously this is a global conversation.

So this idea that there's crypto folks and traditional finance folks is pretty much gone, at least from our perspective and that's great from the Technical perspective so that we can leverage across the board. And there's also this real interplay between those two areas, and they seem to be benefiting from both.

Tom Chippas hit on a lot of that. Some of these are not new, I loved the stablecoin panel. This is not new from sneaker pimps to art to a crypto, it's all the same concept and the same technologies will apply. Execution, collateral management, processing, will this be two separate worlds or a blend? At least from what we've heard today and on this panel, it’s likely to be more of a blend.

Second point it's not the whole chain, it’s not everything on blockchain and life gets easy. It's many different technologies from storage to moving and automating through from here to there. And then, obviously a lot of software that's just about automation, and maybe it's a smart contract or not.

You do not need to benefit from this technology or you do not need to be on chain to benefit from a lot of these technologies. And again, very broad from execution to asset safekeeping which, again, the custody end and then that servicing end we focused a bit more on more last time in previous session with FCM-types.

All the asset classes are in play. There's many

different issues as you get atomic or granular, and there are many different areas for us to all leverage.

So just taking a little bit the journey of our subcommittee and how we sort of got here, you know, there is a lot of relationship between the two. You know, when Gary DeWaal talks about regulation and stablecoin and then makes some wonky argument about swaps and that's connected. I live in the swaps world day-to-day, clearly this idea of this technology could apply to just about anything which is both the benefit and the challenge.

The middle part here on cloud and AI, there are real benefits to this space today. When you start to get this information together and work downstream more a little bit, into supply chain management, there's real AI marrying with blockchains today in the world; energy, maybe in supply chain management, I know IBM is doing a lot that. There’s quite a bit there. And I would argue the “D” of DLT comes from cloud adoption over time versus the blockchain itself.

And again, it's a long-term road but we're deep in it and it's about a 10-year journey we believe.

One thing that's come up for me today quite a bit and the word hasn't been said, but I'll say it here and it's in the deck. So I will force myself to say it. It's the edge.

I read a report a couple of weeks back about the cloud, the edge, and fog. It was really interesting, where the edge is really what is going on with you, on prem with you with you on your phone, in your home. What are you leveraging from the cloud? And that fog, what does that interplay between this pull of centralized cloud-type stuff and decentralized wallets, et cetera?

So all of these are a blend of things happening whether it's widely decentralized, widely centralized, and that middle ground that we're all trying to engineer ourselves to. The reality is that stuff will get much faster in the next three, five, ten years for sure. Through advents in area like in areas like quantum and 5G. We've said it before but it seems to be more of a topic now in the world.

And then, the last point, again, came up a tremendous amount today. Safety, liquidity versus

cost. When you think about what's in the cloud versus what's in the edge versus how you efficiently run information and processing between the two. Data is going up, this cost of storage is going down, the processing power is going up.

There's a massive cost element to all of it and there's an economic impact. We can't lose sight of that. The technology is not just use it and don't care, you have to pay for it. And ultimately, a lot of costs of these architectures are going to drive ultimately what the right answers are, all the way down to a decentralized self-custodied cold wallet or hot wallet.

So exciting times. We're going to pick up on the theme of privacy now. Yesha will pick up there. We'll wander through encryption a bit and get to some use cases.

MS. YADAV: Great. Thank you so much.

Commissioners, Meghan, Richard, it really is an enormous honor and pleasure to have the opportunity to be here today. Commissioner Quintenz, thank you for your vision and leader leadership on the TAC and thank

you most of all to the brilliant staff here at the CFTC for all your hard work and compassion putting this TAC together and making this committee happen. Thanks, especially to Jorge and to Phil for all their hard work and dedication in this regard. Thanks also, of course, to Brad and Shawnna.

So our DLT subcommittee has been extremely excited in exploring the possibility of DLT as a technology that can help safeguard the privacy of users as well as, of course, maintaining the confidentiality of financial markets transactions. What we know in this room is not news to any of us, is that markets have become much more electronic over the last decade and a half. We have seen algorithmic trading become the norm in futures markets our trading floor is a virtual one.

In addition, obviously since the passage of the Dodd-Frank act, swaps markets are slowly following suit. As Commissioner Berkovitz highlighted we're seeing swaps migrate to swap execution facilities, manage reporting, and that has created this need as Commissioner Berkovitz was highlighting for structural

automation in the trading and reporting functions and swaps markets. Really, sort of highlighting the deep electronification of today's derivatives markets.

What this means for us as a TAC is this incredible explosion in digital data that we're facing, that is creating enormous technological and logistical pressure on providers of market infrastructure and regulators to make sure that this data is kept safely, is processed securely, and is stored in a way that makes it impervious to theft, hacking, and other kinds of misuse.

Just to give you some color and idea of scale of this data explosion and deluge that we're seeing in the financial markets today, in the equity markets for example, FINRA has reported seeing approximately 30 to 75 billion observations in a single day, having to store 60 to 70 terabytes of data per month on their cloud. Here in the derivatives market we have, as we all know, seen trading volumes really surge over the last decade and a half.

One provider, for example, the CME saw an average data trading volume over approximately three million

contracts in 2004, that figure is now around 21 million contracts as reported in their quarterly reporting in the 2018. So we really are seeing a tremendous presence of data that needs to be protected and we're trying to find as a subcommittee ways to use DLT as a potential solution to helping market providers keep that data safe.

So there have been a couple concerns that have guided our work in this regard and really affected our thinking as part of our subcommittee. So, the first concern is really the importance of maintaining the privacy of market user’s data. Market participants as we all know really value their anonymity, for many it's a matter of existential economic survival. And so despite the pressures market infrastructure providers are facing, we need to keep their anonymity and privacy secure.

In addition, being preeminent financial markets today, derivatives markets today, this data that we're generating on a minute-by-minute basis is really a singular - - singularly lucrative target for hackers, thieves, and other bad actors worldwide. Really

requiring regulators as well as infrastructure providers to internalize enormous cost to themselves to make sure that this data is properly protected.

Finally our subcommittee realizes that confidentiality and privacy are not absolute values. That in certain context, certain information access needs to be tailored, for example, in the case of the swaps market we can have certain environments in which only certain market participants have access to certain kinds of data. And of course, for the purposes of this room, regulators need real-time access on a continuous basis, in order to perform surveillance and enforcement functions.

So in this context we believe that DLT has the potential to offer some solutions to these challenges that we have identified. In particular, DLT networks can be tailored. They are adaptable. And can suit different information ecosystems. Our normal sort of vision of the DLT network is perhaps highlighted in earlier panels, is really the quintessential vision, is one of open network where any public user can download the relevant software on their computer. But

we also know that DLT technology is developing in a way to make it adaptable and permissioned to allow only certain protected environments to exist and allow only certain users to be able to access that network in a safe and secure way.

In addition, despite being distributed, we can still have single entities stand behind the network in order to help manage and maintain the operations and integrity of that network on a continuous basis. So despite being distributed, we can still have single providers of networks that can help maintain its continuity and business operations.

In addition, the distributed nature of the information on the network as Shawnna’s going to talk about means that we're no longer relying as heavily on single repositories or a handful of data repositories in the market whose loss can essentially create enormous systemic fallout, economic cost, and potential loss of trust and faith in the marketplace. So by distributing information across the ledger, by storing that information in a cryptographic fashion, we're able to reduce essential nodes of information

flow within the marketplace whose breech and disruption can impact all of us particularly here in the derivatives markets.

So finally as Shawnna will now explain, DLT networks are characterized by their ability to encrypt data in a way to look it cryptographically against theft and misuse.

MS. HOFFMAN: Thank you for inviting me here today. It is an absolute honor to be in front of you once again. And two of the fundamental elements, you know, of our human rights and especially our freedom here in the United States are privacy and confidentiality and they are very important. That's one of the reasons we're here to speak with you today.

So, as we're embarking on the fourth industrial revolution. Daily, our privacy and confidentiality are being challenged. We've seen with hearings of Congress lately, and a lot of questions that we do have for each other. So, by its very definition, distributed ledger technology can provide us with a delicate balance of advanced technology combined with security, privacy, and confidentiality.

So you may ask how can a system that is created for traceability and transparency actually have privacy and confidentiality within it? So that's one of the reasons we're going to talk about encryption now. Go to the next slide.

In the age old problem of privacy and confidentiality, you know, of course is seen with the internet each day. Our digital identities, they have many strings of letters and numbers that represent individuals each day. So they're registered with third parties. Now if you really think about it, we're just renting out that information. We're renting these digital identities. We don't have control of them today. That control is in other's hands.

So with distributed ledger technology, or as we know blockchain, it allows for self-sovereign identity. Now the individual has complete control over their data and over their identity with DLT. So by definition self-sovereign identity, we do not need an intermediary. So this means a user's self-sovereign identity can be registered to a claim such

as block on the blockchain.

So cryptography is the process of encrypting data or converting plain text into scrambled text so someone who has only the right key can actually get access to that information. Now blockchain encryption prevents sensitive information from getting into the wrong hands and being misused or even forgotten.

So in decentralized platforms, users can create anonymity and privacy for asymmetric -- with asymmetric encryption. Such encryption system is based on users holding a public key as well as a private key. The keys are unique and the users are mathematically linked.

So one question you may ask is can the encryption be hacked? I know that we've heard about that quite a bit today and those bad actors coming in. You know, I guess the one thing I would like to leave you with, or leave you with one thing today, is one of the big problems that we've seen with technology. The real issue with hacking actually lies in the weakness of the systems that hold the data.

So, simply to say it, it's the in and out of that

data. Now, the issue is not the blockchain itself but it's the in and the out of the data that seems to be causing the issue and that is where the hacking lies.

So as we are looking into the future, we are starting to dive into other areas just to see what we can do to secure that data to make sure it still is, of course, providing privacy and confidentiality.

We have on the horizon, of course, quantum computing coming down the line. And companies like IBM are working on quantum encryption. And what that will allow us to do will simply use principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked thus providing greater security and privacy to the individual.

So DLT is also known for its ability to create an encrypted and immutable digital record of transactions. Today the most widely used hashing algorithm is SHA-256. And that hashing algorithm can convert data into encrypted fingerprint that represents the data’s digital signature. So SHA-256 represents a one-way hash, that means it's impossible to reverse engineer and retrieve underlying data in

that original form.

So this helps protect data's integrity, so if this underlying data is changed in anyway a new hash is generated.

So DLT can thus enable efficient storage and also filing of documents. Once a transaction is concluded, the hashed fingerprint represents a trusted and immutable record for the network. Nodes within the DLT network maintain the hash digital fingerprint of transactions rather than a vast quantity of underlying trade data. Underlying documents such as swap contracts or a warehouse receipt are maintained elsewhere like a secure cloud-based system, such as peer-to-peer distributed file storage system.

And now we'll go back to Yesha to talk a little further about DLT and custody.

MS. YADAV: Thank you Shawnna. So our DLT subcommittee has been quite excited and enthusiastic about the potential for this DLT data verification and information protection technology to be useful in the custody function in financial markets. So as Chris and Tom's presentation earlier showed, custody is very

much a critical pillar of the financial markets today, and perhaps nowhere more so than in the derivatives markets.

Derivatives markets are responsible for the transfer of literally trillions of dollars' worth of economic value constantly.

In the commodity space we're seeing warehousing and transfer of incredibly important commodities such as agriculture, livestock, food stuffs, precious metals, and so on that are warehoused and transferred in accordance with determinations made in a derivatives market.

For the financial assets, trillions of dollars' worth of securities and cash are moving as part of the underlying derivatives markets trades themselves as well as part of collateral management that attaches to those trades. So for us as derivatives -- sort of nerds, custody is really an essential part of what we do in making sure that function works as securely and smoothly as possible, is a central concern.

So here we feel that DLT technology can be particularly useful. In particular DLT networks that

are able to securely certify user identities using the digital identities using digital identities that Shawnna was referencing, verifying trades by references the ledger that exists at a given moment. And then, automating signals to custodians and warehouses to direct the transfer of assets represents a way to fully automate the custody function in today's derivatives markets.

Now we're already seeing as alluded to earlier, warehouse receipts that are becoming more electronic but still enormous uncertainty remains and a lack of coverage remains that means that assets cannot easily be tracked, they’re not necessarily as liquid, not as easily to sort of see where they are in the supply chain given the sort of lack of real-time tracking of those assets in some context. So here by using DLT technology to verify data to securely transmit transaction information to custodians and third-party warehouses, to then direct the transfer of those assets we can hopefully automate this function more fully and potentially make it more efficient and more sort of useful for growing derivatives markets looking

forward.

And now Shawnna will talk about further applications.

MS. HOFFMAN: Thank you. So, next we wanted to talk about audit and compliance. So blockchain can be an absolute game changer for audit and compliance.

So today financial data as we know is dispersed within firms all over the world and so the biggest challenges, of course, with audit and compliance are the needs for indelible record that records the key of transactions over a reporting period.

So DLT-based networks collect transactions of records from a diverse financial systems. The append-only and tamper-proof qualities of our DLT create high confidence financial audit trails. Privacy features ensure only authorized users access. Consequently, this can actually lower cost of audit and compliance by a tremendous amount.

So importantly regulators can have access to that data on a as needed - - on a live, as-needed basis at any time. So initially we are seeing the assessment of financial statement assertions such as existence

occurrence, accuracy and completeness of information are amongst the prime candidates for blockchain and audit automation. Next slide.

So here we have an example of a use case that focuses on consensus. So any reference data that is shared in a business network is potential blockchain network. So we start to see each participant maintaining their own codes, within a permission DLT network. The network can create a single view of the entire dataset - - dataset - - to those who are given access to this data.

So think about it this way. Claim or identity information is required for fraud prevention or insurance networks, you know, is a great use case here. Also think about it in the aspect of banking. So bank routing codes are common vocabularies for asset exchange data, where it’s more important to make changes to the dataset in real time and without requiring a trusted third party.

And here we have an example of a use case that focuses on finality. So as we know letters of credit is a centuries-old process started in Medieval times

with the Knights Templar who required a way for pilgrims to travel to Jerusalem without the danger of carrying money around. The letter of credit process is difficult one to automate due to the sheer number of network participates involved. Blockchain gives us the opportunity to modernize the letter of credit process. With blockchain the letter of credit is stored in blockchain and once spent is marked as spent so the value of the letter cannot be spent again.

Again, no double counting.

So the use case also allows for innovative methods of payment using internet of things. So for example, smart contracts could be implemented, implementing rules that prevent, allow access, reduce payments if certain conditions happen. You know I have one client that we're working with which is fascinating, and we built out a program that allows that if you move -- if the ship moves into a certain zone, that payment would automatically occur through blockchain. And so, we're starting to see major advancements in regards to GPS, in regards to tracking, in regards to automating many of those

processes and it's only with blockchain that that capability can happen.

So we do have ongoing questions for you all, but I would be remiss not to remind us, all of us, that technology rapidly changes. Therefore it is important not to regulate the technology itself but also the outcomes of the technology and how it affects the individual.

You know, we would be absolutely remiss to have any sort of regulation that is specific on technology, because I will promise you tomorrow the name and the nature of it will change.

So, our four questions here, we'd like to read them out. Do DLT-based information verification standards meet various legal standards for data, privacy, and security in derivatives?

The next for interoperability. Will market demands just -- will markets -- there we go, demand just a handful of encryption standards?

Third one down. How should innovation and encryption take place where a handful of standards support financial markets?

And then, should the CFTC lead international standard setting in relation to data privacy and DLT?

CHAIRMAN GORELICK: Great. Thank you very much. We're going to up for questions. I will start by throwing out a question to the group.

I'm wondering given Brad's timeline that he discussed of 2025 being the likely arrival time of many of these advantages, what do we see, I'd like to hear from each of you, the short-term developments the Commission should be looking for in the next year or two that you're most excited about?

MR. LEVY: Yeah, and I'll just pick up on the general point maybe which is I would say 2025 is the time where many individual value props will come together and create sort of this super value based on this new technology space. Along the way, there will be real value created in individual areas that will then over time begin to connect with each other, and one plus one will begin to equal four, five, ten; but in the next several years it will begin to, you know, really add quite a bit of value.

Shawnna, I know you have real world applications.

I have a few myself in terms of what people are doing today. You know, maybe it's analogous to the financial system or actual real world, but there's definitely use cases today that are providing incremental value not changing anybody's life but real.

MS. HOFFMAN: Yesha, go ahead.

MS. YADAV: Great. So thank you for that question Rich.

So one of the -- sort of paying off that, so one of the big issues in this space in the near term is the lack of standardization internationally. What we know with respect to derivatives is that these markets are quintessentially cross-border, and just taking the US and the EU as an example, we know that privacy standards, data storage standards, data transfer standards vary enormously between the US and the EU, and consequences for violating those standards can be severe.

So in that marketplace, in the absence of standard setting, and the absence of cross-border cooperation, to set some framework under which this

technology can be developed, the risk here is that the use cases that we're highlighting remain quite bespoke. That they are restricted in ability to scale and that really is a problem to the extent they represent real value propositions for the market overall.

MS. HOFFMAN: Well, and I think if I was to make a suggestion, it would be to look not at the technology but what is the outcomes that we want? What are the human rights that we want? What's the freedom we want? What's the privacy and confidentiality?

Look to those and the technology will fall into place. So I think that would be my suggestion, because as we start to jump down the line of creating standards and creating procedures, and hopefully regulations that make sense for the market, you know, we start to look at things internationally, we have regulations all over the world that really do compete with each other and we don't want to regulate our businesses here in the United States to be regulated out of being successful and being the top businesses

in the world.

You know, do if we look at those fundamental rights versus the technology, as you start to put those standards in place, I think that would be one of the smartest things we could do.

MR. LEVY: Yeah, and just one area -- a couple of areas specifically, we definitely see the potential for DVP-like initiatives in existing trusted private networks that do things already. So there's definitely areas that we think will start to come in the next several years there, not five years out.

I would say less cross-border initiatives. I think that's just a bit of a nest of challenges, whether it’s privacy laws or technology or politics, so I would say those won't occur necessarily, although a lot of cross-border payments and all of that also is certainly a big deal globally.

And just general record safekeeping. To a lot of the comments made on compliance, how do you prove you've done something and then how do you go back and deal with something when you know you have to resurface it? And then obviously, custody. Those are

real -- in the next one, two, three years, there will be real value in those areas and we're involved in some of those initiatives ourselves.

CHAIRMAN GORELICK: Thank you. Alex.

MR. STEIN: Thank you. Excellent presentation. Mainly for Shawnna, but please everyone speak up.

You raised privacy several times and encryption. What are the best practices in anticipating the power of quantum computing because in a public -- publicly readable DLT, people may feel overly confident that today their data is not accessible but with the advent of quantum computing it's all there.

MS. HOFFMAN: That is an excellent question and one that keeps me up late at night.

I don't know if I even have the answer that you're looking for. But as we're continuing to develop quantum encryption, we are having other companies that we are seeing in the marketplace also doing the same thing. As much as possible today we do recommend quantum encryption even now. Because there’s going to be at some point, that some bad actor is going to come into the system that has that

capability and really wreak havoc around the world.

So not only even just when talking about blockchain but talking about anything security-wise.

MR. STEIN: Thank you.

CHAIRMAN GORELICK: John.

MR. LOTHIAN: What are you seeing in terms of the interest globally in terms of investments in this area? I've heard stories that because of the ambiguity of our regulations, because of all the maybes and the like that a lot more venture capital firms, DLT projects or cryptocurrency projects is happening overseas than in the US and that it's more like prove the concept overseas and then bring it here once we know how to navigate the regulation a little bit better.

MS. YADAV: I think there's a lot of variation in international responses, and some jurisdictions have been forward relative to others.

For example, in the case of certain Asian countries for example, Hong Kong, Singapore, they have set up sandboxes to help. Australia, as well has Sandboxes to help test nascent DLT-based and FinTech

technologies with the view to sort of seeking real world reliability.

Other jurisdictions have been slower in the uptake or at least more cautious. In terms of sort of looking at the overall picture in this context, I think that's one of the difficulties in trying to navigate this space. Different countries just have different attitudes towards innovation.

In the case of crypto, for example, we've seen China ban it, India ban it. Whereas other countries have been more responsive. And part of that may be that certain financial systems just need these technologies more.

And one can imagine, for example, DLT for custody working really effectively for cross-border trades where there is no trusted intermediary in-between, where the swaps counterparties can instead rely on a DLT-based system instead on relying on an intermediary what may not exist and they may not have enough trust in each other.

So where trust is lacking, these systems can be much more palatable to regulators and to the sort of

financial population but again, this really varies by jurisdiction, that's a challenge of being in the space.

MS. HOFFMAN: I just want to mention one thing. So what's fascinating about the countries that have made it so that no one can use crypto, you know outlawed it. These are the same countries we're working the most with when it comes to blockchain projects for business. And so, when we start to look at the blockchain for enterprise, you know, no on crypto, but absolutely yes on blockchain. So that’s fascinating too.

MR. LEVY: Yeah, that's a great point.

I would say this public/private element is really important, a lot of what you see internationally is driven quite a bit at that public -- state sponsored. And I would say it’s not as much a blockchain DLT as it is around quantum, cyber, AI, and robotics. And then, how blockchain fits into that much bigger picture. My guess is the US, itself, specifically is doing quite a bit on those fronts. Some we may know, some we may not know, but outright sort of distributed

ledger blockchain, venture capital-type initiatives, interesting.

I would say the bigger play is that much bigger state/private, you know, there are some countries that are very specialized in cyber, you know, for example -- you know China's got a whole plan for 2025 that they are pushing toward around all those technologies and I would say blockchain just sort of fits within that frame.

CHAIRMAN GORELICK: Thanks. For the last question I turn to Erik.

MR. BARRY: Sure. It's very enticing to look ahead to 2025, and a DLT network has solved four data privacy concerns: for encryption, for consuming machine readable regulations, for smart contracts; but if we look down to an alternate universe in 2025 and one CCP has chosen Hyperledger and other chosen Ethereum, and others chosen Corda, DAML, all these different DLT providers that are active in the FinTech space.

I'm curious what recommendations should we be providing to the Commission to not only lead standard

setting internationally, but also between these different iterations of networks between different players in the industry, without selecting a single solution that, you know, play the role of a king maker, but also balancing that interoperability?

MR. LEVY: Yeah, maybe it's a focus on what you want to solve for, the risks. What you actually want it to do first, that's come up a number of times today.

Pay attention to everything. There's just sort of that education element. And then ultimately, there will be many, many. There's very unlikely to be one. People talk one, but it almost never lands there. And there will be four, five or six that develop globally and in each area with specialties, and there will be interop that will make sense over time.

We've always talked about interop and fungibility, it's a futures concept. It never goes all the way there but it gets sorted out or filtered out over time based on people really knowing the problem you're solving and then solutions coming there and, you know, the momentum going behind the solutions

that are winning and those would tend to be pushed to interoperate maybe or not, depending how the world evolves.

MS. HOFFMAN: Well, and I think it's no different than us looking at the cloud or any other technologies that we've had that are more centralized. You know blockchain it’s fancy, it has a lot of hype right now -- or distributed ledger technology, whatever we decide to call it in the future. You know, again, then it comes down to the results and what are the results that we are looking for? And really, what are the results we're not looking for? What are those results that could cause havoc in the marketplace and cause havoc for the individuals? You know, again, I would never say -- I would never recommend to, you know, put anything forth in regards to technology itself, but more towards the results.

CHAIRMAN GORELICK: Okay. Thank you, everybody. We'll take a break now for lunch, and return at about 1:30 p.m. Thanks.

(Whereupon, at 12:42 p.m., a luncheon recess was taken.)

A F T E R N O O N S E S S I O N

(1:34 p.m.)

MS. TENTE: I'd like to call the TAC meeting back to order and turn the agenda back over to Richard.

CHAIRMAN GORELICK: Thank you, Meghan. I would like to turn to the next panel, in which we'll hear from Alicia Crighton, the Managing Director at Goldman Sachs, who will be presenting on behalf of the Futures Industry Association on best practices for managing risks associated with automated trading systems and highlighting FIA's best practices.

Then we'll hear from our fellow TAC member Mayur Kapani, Chief Technology Officer at ICE, who will speak about the risk controls for automated and electronic trading employed on ICE. Alicia and Mayur will be joined by fellow subcommittee members Yesha Yadav and Ed Prosser, Senior Vice President at the Scoular Company, to contribute to the discussion after the presentations. We will then open it up to our broader TAC membership to explore next steps for the subcommittee and its work and with that, I will turn this over to Alicia.

MS. CRIGHTON: Thanks very much, Richard, thanks to Commissioner Quintenz and to your staff and to the subcommittee for putting this important topic on the agenda for today. You all have a copy of our updated materials. I'll be using this as a primary context for our discussion today.

So with that let's get started. Electronic trading has become an integral tool for an increasingly large percentage of the market participants. So all of the principles we reference here we think should equally apply to human and automated trading, or manual and automated trading.

As we've all recognized in talked about the benefits over time of the speed, the efficiency and ease electronic training has made it attractive to the full spectrum of organizations and individuals that interact with our markets. The wide spread adoption of electronic trading, including automated trading systems, has provided a range of benefits, not only liquidity and tighter spreads but it's also created the need to continue to update risk management practices on a continuing basis. And that's where

we'll really focus the context of this conversation.

So in terms of the agenda for at least my comments today, we'll spend a few minutes on the evolution of risk controls, while the FIA work has predominately focused on futures, I'll bring and little bit of context from the options and equities perspective, given my role at Goldman. And we'll spend time walking through best practices in regards to exchange risk controls. FIA has published extensively on all of these topics, so we'll spend some time going through the principles we've published and advocated for. What the pre-trade controls look like and what the post-trade controls look like and how the ecosystem should function.

We've spent a lot of time and effort publishing and conducting surveys, so we'll talk through trends and themes from those surveys and then we'll go through what we think are areas for continued development and where we go from there. So we go to the next slide.

We talked through what FIA's role in the evolution of exchange risk mitigation practices has

been. I think this timeline is really helpful in terms of the context of the work that FIA has done. FIA has engaged with futures exchanges, market participants, and international regulators for nearly a decade on the development of best practices to mitigate the risks of electronic trading.

If you note on the slide here, in terms of the timeline and I'll highlight just a few different items, it's quite dense obviously in terms of the activity. The top of the timeline shows the actions that FIA has taken, the bottom of the timeline shows a number of different market events.

A couple items that I will call out here are one, the FIA market access white paper which is actually where our timeline starts. That was published in April of 2010. And if you notice, we actually put out that market access recommendations prior to the Flash Crash.

A few other items I will call attention to, are the Drop Copy white paper in 2013. Also in 2013, the FIA response to the CFTC concept release on automated trading and the March 2015, the guide to the

development and operation of automated trading systems.

We moved to the next slide to get into some of the a depth that FIA has published. We kind of start at a higher level on a more principles-based advocacy effort and really the kind of driver there has been centered on the belief that in order for risk controls to be effective, they should be principles-based rather than a prescriptive set of requirements which can become obsolete as markets and their participants evolve.

I think two risks that are worth highlighting from the kind of prescriptive comment is one, I think as we've just said, they become outdated quite quickly. And two, the cost of implementation particularly in an already constrained environment can be quite challenging for participants to absorb, which is why we think the principles listed below, and we'll step through them in a minute, are much more effective and give the industry the ability to be nimble.

Walking through what the principles are. All electronic orders should be subject to exchange-based

pre-trade and other risk controls. Exchanges should provide tools to control orders that may no longer be under the control of the trading system. Exchanges should adopt policies to require operators of electronic trading systems to ensure that their systems are tested before accessing the exchange. And the last principle, exchanges should be able to identify the originator of an electronic order and whether the order was generated automatically or manually. So that's kind of the high level principles.

Moving to the next slide. We go through a series of pre-trade risk controls. Really the intention here is to have the pre-trade controls work very closely in tandem with the post-trade controls. While we've advocated for this set of controls, what I thought would be helpful is to lay it out in a chart format as well, to show across a number of different line items, what the participation should look like across the various participants in the life cycle of a trade.

So it's not a single ownership to a particular participant in the life cycle of the trade. For many

of these different line items, we take the view that each of the participants should actually have a bigger role in that kind of particular check.

Again, we think these pre-trade controls can be implemented at various points in the execution order flow at the trader level, at the broker level or at the exchange level. And all of these controls are critical in preventing a market disruption.

We think these then are closely aligned with a series of post-trade controls, which are then more designed to protect a credit event. So again, a smaller list but focused on the trader, the broker, and the exchange. If we look at Drop Copy reconciliation, post-trade credit controls, exchange era trade policies, and a robust audit trail. And again, all of these really tie to the principles that we laid out earlier in the materials.

We switch now to the surveys. Since 2010 FIA's conducted a number of different surveys of exchanges, as well as market participants, including clearing firms and principal trading firms. Surveys were completed in 2010, 2013, 2015, and 2018. Again, all

of those are referenced on the timeline and you can see how they interact with different market events.

Exchanges were surveyed on their provision of risk controls. And market participants were surveyed on their use of the FIA recommended controls and there are a few high level trends and themes that we actually wanted to highlight in terms of the information that's been provided to us throughout the course of these surveys.

One is there's been a substantial increase in the implementation of market integrity controls since 2010, including price banding and exchange market halts. There's been a steady upward trend in the adoption of basic pre-trade controls such as order size and net position limits. Number three, controls and tools such as self-match prevention, Drop Copy feeds and kill switches are widely available. Number four, there's been a steady upward trend in the voluntary adoption of controls across the various participants in the life cycle of the trade; including traders, brokers, exchanges, and clearing firms, and generally there's been positive feedback to industry

initiatives and responsiveness to identify and self-solve industry risks.

On a more granular level we wanted to share some feedback that we obtained from market participants through these surveys as well. Specifically feedback from the traders included that there's broad use of some of the following controls: pre-trade max order size limits and data reasonability checks, some form of self-match prevention, message and execution throttles, and Drop Copy functionality. And clearing firms that were surveyed indicated abroad use of the following, and these were either internally or those that are offered by an exchange and that will vary based on participant access, but they would also be using message and execution throttles, price collars, maximum order sizes, order trade and position Drop Copy, and order cancellation capabilities.

So from a continuing development perspective, we feel that as markets and risks continue to evolve, the industry response to the risk present is also evolving and FIA’s identified the following themes: One is increasing automated access to exchange risk controls.

Initiatives are underway at most exchanges to develop API access to the various risk controls. More granular pre-trade risk controls. The industry is working towards developing more granular controls, specifically referencing either an account or an individual trader level.

Potential introduction of new types of limits. Review is underway to determine the applicability of a buying power limit, kind of the concept of a client credit worthiness. And certification and testing. Industry efforts are underway to work with exchanges to improve the functionality available in exchange certification and conformance testing environments.

So I think that really leads us to sort of what's next from an FIA perspective. I think, you know, it's a good time to really take a pause and look back on kind of the 10 years' worth of industry work that have gone on in terms of the surveys, the white papers that have been published and all of the data that we've been able to glean to say, okay, we have this data. What is the right way to -- what is the right next step in terms of moving that data forward?

Markets have evolved, participants' access to markets have evolved. We have a tremendous amount of data that we've collected over the last 10 years. What's the right next step in bringing those pieces together? So I think across team at FIA we'll be spending some time thinking through what do we do next? Is it an additional survey? Is it a white paper? Is it a letter kind of summarizing the views, the standards and having a more open dialogue around those.

I'll pause there.

CHAIRMAN GORELICK: Thank you Alicia. We'll turn to Mayur for his presentation and then do questions together at the end.

MR. KAPANI: Good afternoon everyone. Hopefully I'll try my best to keep everyone awake. And so, first I wanted to thank the Commission and the Commissioners and the TAC for giving us this opportunity to share our experience building out the risk controls. And I'll be continuing on the theme, which Alicia kind of highlighted. We worked hand-in-hand with the industry, with the FIA and every time we

got some form of feedback where as an exchange we could do something better, which would help our customers and get our clearing firms more comfortable in how they manage risks for different group of participants.

We took the feedback at heart and have continued to evolve as our thinking has evolved as the markets have evolved. And what I'm going to share is going to be the current state of the union in terms of how we think about risk across all futures exchanges and also how we see where the future is going, which is which is completely in line with the way FIA and other industry groups have thought about it going forward as the markets are evolving further.

I just wanted to give you a sense of our risk controls philosophy. And this is just a short set of principles we kind of think about internally when we think of risk controls across all our exchanges. And when we talk about all our exchanges, we are jurisdiction agnostic. So we look at ICE Futures Europe, ICE Futures US, which focuses on our soft and financial products, ICE Futures Europe that focuses

heavily on our energy products and our interest rate products. And our energy division in the US and also NDEX, which is based in Netherlands. So when we talk of risk controls, we look at all jurisdictions and tried to come up with a super set of risk controls such that any individual jurisdiction that has any kind of a rule or expectation, we are matching it for all our exchanges. And this also gives a singular view to our participants and they know that when we build something, we are building it for all and applied to all our exchanges.

The other philosophy we push internally is we should think really hard what we can do, preventive measures versus reactive measures, where preventative measures are what we can control pre-trade and what we can detect and mitigate after an event has occurred, post trade. So focus on prevention along with post-trade mitigation and detection.

Another piece we heavily internally, we know there are trade-offs in terms of throughput and the latency and all the other things which our participants care about. But we keep real-time

management as a principle as much as possible. So that -- so that we don't compromise on risk management compared to the other drivers. So as far as the priority is concerned, we try to focus on real-time management rather than then batched or a post-trade management.

We tried to get it to our broad set of participants. So we try to keep a granularity of controls at different levels. Be it user account, desk, which is essentially a group of accounts, and the whole company or the trading form. So depending on the products and the risk stance different participants have and sophistication they have, they can choose these levels of controls.

The other thing we focus heavily on in terms of building out the tools and APIs such that we have a tighter integration with the third-party systems and in-house systems and in-house systems could -- our consumer could be a clearinghouse, which is getting real-time feeds off of these risk triggers along with the participants, themselves.

So we focus heavily on tighter integration such

that building out APIs and building out frontends such that we have much tighter integration with third parties and other risk systems.

Now getting into the specifics, I know some of this might be a repeat based on what Alicia presented earlier, but I felt that it's important how we think about risk controls in different categories and this particular set of risk controls which we have are market level risk controls. You're where we configure these controls and set up these controls at individual product or a market level such that we prevent orders with prices outside of certain bands.

And we have both soft bands and hard stops where soft bands, we give a warning to the customers submitting the order saying that you are submitting an order outside of this band. And we informed them so that they can take appropriate action or make sure that if it is intentional there and they're okay with it, they leave it in the market. So we give warnings on soft warnings related to the price of the order they have submitted.

We also have hard stops where customers cannot

order, send orders outside of certain bands for a given market. This is just to avoid erroneous trades where they might be, they might think that entering an order for one market but might be entering an order for a different market and protect against those kinds of erroneous trades. And we have many kinds of those price controls which are managed by our market supervision and are configured at a product level.

The next big investment we made based on the 2010 Flash Crash was building out a circuit breaker where if a price of an instrument moves beyond a certain higher or lower -- beyond a certain band in a small period of time, which is configurable We pause the market and when we pause the market, we are telling the -- especially if there are runaway stops or if there are orders coming in which are being triggered based on this quick price movement in a small period of time, we hold the price at a given interval and also let the market absorb the event and then reopen the market.

If the market is directionally going in the same direction, we don't stop it, but we kind of pause it

for a period of time and we call this interval price limiter or a circuit breaker. And this, and I'll speak more about it, but these mechanisms helped us a lot during the Saudi bombing event that occurred a few weeks back and I'll go into some more details in the latest slides.

The other things we have is we have a concept of a no cancellation range where if we see a trade being done outside the range of what we call as a anchor or a base, which is based on the last traded price and how the curve is for the product. We kind of inform operations, “Can you please make sure that this trade looks reasonable and there is no issue in the way either our settings or the way this trade was conducted.” And they just take a look at it and review to make sure that there was nothing untoward when they observed that kind of a trade at that price.

Then we have protections against somebody overwhelming the market with messages or orders in terms of per session limits, per user limits where if we get orders outside a given throttle limit for a given session, we prevent more orders to come in. And

we have sophisticated mechanisms such that customers are allowed to cancel their order, but they are prevented from submitting new orders, that way we let them manage their risk more effectively by getting out of the market while also protecting the market -- the integrity of the market where things are being executed.

One feature which directly came about based on the feedback from the industry participants was ability to manage their risk when they -- either we couldn’t reach them or they couldn’t reach us in terms of connectivity. And as soon as we detect it, as soon as we detect that we pull all the orders on the market just to prevent a trade, which was unexpected. And this feature has been extremely popular and we've made it as a standard feature where people don't have an option to even opt into it.

The next set of participants, the next set of controls are what we call as a clearing member or in equity parlance, broker managed controls where they control what kind of limits they want to give a participant based on how they believe the risk of that

participant and the sophistication of that participant. So we have ability by which the broker can or the clearing member can set the max order clip size a participant can submit. How many working orders in terms of sizes the participant can submit. Net positions this participant can take in any given product, product group.

We also have a limited, even though it's not very popular, where independent of them sending orders on both sides of the book you can be limited by, you don't want this participant to send too many buy orders, so you don't want this participant to send too many sell orders. So we have limits for those.

And then there are some new limits we are introducing. Separate limit for off exchange clip size limit. Where if they are submitting a block trade, some clearing members told us they wanted better control of what is the max block size that can be submitted for a given participant. And since this has been an evolution and we support a large number of products, there has been always a push for more granular control of the product groups and which

products they want participants to trade and which products should be included in a given product group. So we continue to evolve this facility for our participants.

So all the limits I talked about are all pre-trade. And the next stage of the evolution we are going through is looking at what is called as a margin limit or buying power as we had mentioned earlier. This is maximum dollar amount across all products that are traded on the ICE Exchange. For a given participant, what is the maximum dollar amount we want this participant to be held to as a limit? And we've invested heavily over the past few years to build that out.

We started at the account level and we are getting quite a bit of a push from our participants to evolve this with a group of accounts where a limit can be set at the account level. A limit can be set for a group of accounts or there can be another limit that can be set at the trading firm level. And if any of these trip we want -- they want notifications at different thresholds; 50 percent, 80 percent. All

these different thresholds where a clearing firm want to be notified of breaches of these dollar limits. And in some cases have actions available to them such that they can hold new orders from coming in for these accounts. Potentially even restrict any trades in a given set of products.

So they want all kinds of granularity in which actions to take based on these limits for an entire portfolio of products that they are trading at ICE and we continue to invest. And I've put some dates where some of the functionality is being rolled out later this year and early next year.

In addition to the clearing member managed controls, we also have some controls which we provide all the visibility to all the controls that have been set by a clearing member to the trading member. But trading members themselves have asked us for some controls which are very specific to them. One of the big ones is self-match prevention where they want to be able to send orders and the exchange manage the fact that if this order is matching with another order on the book from their company or one of the other

users of the company or a desk in their company, they want to prevent the self-match.

And we've been building this tool for a few years and we've seen a lot of adoption of this particular prevention and we give all the management control of this to the trading firms.

In addition to things which I talked about, which are pre-trade/post-trade, there are a set of controls where market makers who do high volume option options market making have asked us for a set of controls where they want to manage risk, where if they do a set of trades in a small period of time as measured by the volume of trades they've done, the delta of the options they have traded and there is another one which we call cumulative, where they do a set of trades across a set of the instruments for the same product group.

We allow them -- we automatically pull their orders so that they're not exposing themselves to too much risk. And this is one of the ones which again, used by all our options market makers because of the nature of the instrument and the way options trade.

In addition to the controls themselves. That is one area, again, we've invested heavily in terms of making sure that the detection and mitigation of breaches is as much a part of our workflow in addition to actually implementing the controls at the venue level. We have evolved and added a huge number of visibility and kill switches in terms of controlling user sessions, withdrawing orders, disabling accounts, changing limits dynamically such that our trading and clearing firms feel that when there is an untoward event, they are able to manage the risk appropriately.

We're also investing heavily in improving this visibility and also adding a lot more flexibility in terms of selecting a set of filtering it by selecting a set of products or selecting a set of accounts that should be impacted based on quickly allowing them to set those configurations with these kill switch kind of features.

We have -- as everybody here has raised this a number of times, is it's important that not only we provide tools which are a frontend and or GUI-based but we also provide APIs through which firms and

vendors can integrate all these risk controls into their own workflows. So we've invested heavily in building out the risk management API. If you've build out separate order and trade call drop copies for risk management and reconciliation, and we continue to evolve adding more features to this - - our API set.

Last but not the least is breach alerts. We want and continue to evolve different delivery mechanisms for these breach alerts being a frontend screen, which has all the breach alerts. Email, which needs to go to a set of participants based on a certain breach alert. And we've invested heavily in and continue to invest heavily in improving this part of our platform.

So this is how the risk controls look like. And I wanted to give a taste or some view on how well did these risk controls perform when we had the Saudi bombing event I think on the 11th of September. So one of the things, and I've broken the slides into three, one is how did our price collar sell? And what happened?

This is not a very interesting chart, but this just tells you that when the Saudi event happened,

there was a lot of uncertainty and lot of volatility in the market. And just to give you a flavor, as soon as the market's opened the price jumped 20 percent until it stabilized, I think around 10 or 12 percent within the first half hour.

And there were a lot of participants who are sending orders across the curve, which are way off market. So we were preventing all those trades and erroneous rates from occurring with these controls and they were very effective that day. And most of these controls and I got a question earlier whether if these controls -- can you show us during the whole day how they fared. What really happened was in the first half hour we saw large number of controls, price controls got triggered because the market was not sure where it was and there were people were trying to do a lot of things which, and the markets are moving so fast that they were not able to keep up.

And during this time also we discovered we hit our circuit breaker only once, but we hit our circuit breaker, which is set up where if a price moves a dollar within five seconds, it pauses for five seconds

before it lets the market move again. And I think, at least in our books, these controls work very effectively and worked as intended with no negative consequences, which we heard either from the industry or the participants. So we, in our books, they worked really, really well on the price control side.

The next one is how did, and I got this question from I think Commissioner Quintenz's office, is how did the credit risk controls work? What was interesting to me at least, was that they worked, we didn't see anything unique in the credit controls because already the market and the industry had evolved where these controls were set at appropriate levels, where we didn't see them trigger particularly in an different way or an interesting way on that particular day. And I just, I've taken a sample set of our pre-trade credit controls and shown you guys how many times we triggered.

So as you can see, these numbers are really small and this is BAU, business as usual for us. And there was nothing interesting about these controls themselves. They work. The clearing firms, the

trading firms, all the firms who trade market like this are very evolved and they have already leveraging all the controls we have developed. So, that particular day was not very interesting for us.

The last but not the least, was Brent Crude options. Again, as you can see, it was BAU, business as usual for us. And what you see on 23rd, 24th, is actually an interesting part where one of the participants had an issue where the way they were coding was not appropriate. So to their -- what they expected how the market to behave and they were hitting their own triggers and we were just informing them that you are hitting triggers. Again, it is nothing untoward. This is a normal for us more like a BAU kind of event. And there was nothing in the Saudi bombing event that completely changed anything there.

And the Saudi bombing event, the main thing we started, we saw was the way the price collars worked and the price protections. That was really beneficial because we didn't have any other trades and the market was very orderly. And we were very pleased with the outcome.

With that, I'll pause here and take more questions from the panel.

CHAIRMAN GORELICK: Okay. Thank you. I'll ask a quick question and then I'll turn it over to anyone else who's got questions here. So one thing I noticed Mayur was that you talked about price banding on the one hand where you will reject orders outside of a particular price band and a no cancellation range. I'm wondering whether those are the same ranges or whether there is some gap between them such that there are orders that are outside of the price bands but that would be canceled.

MR. KAPANI: So no cancellation range. I mean this is, Richard, if I answer the question for -- if you take across all our products, the answer is it depends. In many cases, non-cancellation range and the hard stops are the same. In many other products where there is a small gap between a no cancellation range where the markets are more illiquid and there is a possibility that we might get those orders and they might be legitimate orders. So non-cancellation range might be inside the hard, what we call as

reasonability limits.

So it, it depends on the product but usually they are the same but they will move based on the nature of the product.

CHAIRMAN GORELICK: Okay. Thank you. I'll start with Brad.

MR. LEVY: Thank you. In terms of the types of technologies you may be leveraging and when you get into breach and things that are looking like an issue, is there initiatives that you are driving or you see on the horizon that are really more predictive? Like something isn't really clearly an issue but something looks like it's building up. It's not technically violating any kill switch or it's a breach buffer, but it's just more, more future tech predicting something that's looming or coming forward that you can't quite see based on, you know, a Flash Crash --

MR. KAPANI: Yeah. I mean, this is a very interesting question and obviously that our market supervision team will give you a lot of details on how they think about this.

But what we do is we -- and for predictive

analysis, the key part is you need to have is you need to have a historical view on what is good and what is what is considered an outlier. So we invest a lot of time in processing our historical data to form a view at different levels. We might form a view at the market level or participant level or even at a same where two counterparties are trading with each other.

And again, we are getting into a lot of market surveillance and supervision and we have alerts which highlight on the screens of our market supervision teams, which we give them exceptions which are outside the norm, be at market level and sometimes a behavior of a given participant in a market level and let them form an informed view and decide whether it is a serious event or a non-serious event.

I don't want to call it AI yet. It's more statistical based on the kind of tools we have built. It's predictive in terms of looking at history and trying to see what it is.

And as you can imagine on the Saudi, the day we had the Saudi bombing event, everything was going crazy. So we, at that point in time, our market

supervision was closely monitoring all the limits, closely monitoring all the movements we were seeing. And at least most of the time they said, okay, this alert based on the nature of this event is acceptable. And they would, they would move on. They would not -- they didn't do anything unique except for saying that are these bands appropriate? Are our configurations appropriate? Should we be thinking about changing them?

So they had -- that's the extent to which they kind of touched the market. But outside of that, they didn't do anything significant.

CHAIRMAN GORELICK: Thank you. John?

MR. LOTHIAN: You had another market that in the last week or so that made a significant move down 16 percent in a day. And that was the Bakkt Bitcoin futures.

MR. KAPANI: Yes.

MR. LOTHIAN: So that's a lightly traded market, 72 contracts that double -- on the first day doubled or more than doubled, 166 on the second day. Can you walk me through what may have triggered that day in

terms of your circuit breaker controls for something that's illiquid like that?

MR. KAPANI: Yes. It's interesting, the circuit breaker controls is a movement of price a given price in a very short period of time. That didn't happen in this particular Bakkt market. Right. So, and you probably have some more details. We had a spread of -- - so our minimum price increment is $2.50.

So we had a spread from $2.50 to $20 in the spread itself as it was being quoted. So as this market moved and traded, we didn't see sudden jumps or sudden -- where it would trigger any kind of a circuit breakers, but what happened or helped and we didn't have enough liquidity to say whether these rejects were just errors or rejects because it's people are still trying to find the market, but our price collars worked as design. Which is basically we are not letting orders go outside of the price collars. And the other thing, since we are a new market and many of the clearing firms were uncomfortable or worried rather, that we shouldn't have a runaway guy trying to go and buy a lot of stuff which he is not prepared

for.

So had set limits appropriately based on the capital or the liquidity of that participant. And those holding all those things worked as designed.

And one of the things which at least from my perspective when you look at a market like Bakkt, a new market, highly volatile, these controls which we have built and this industry has evolved over the past maybe 20 years in terms of building out these controls, really helped a market like that to evolve in an orderly way. And I think it really helped there.

CHAIRMAN GORELICK: Chris?

MR. HEHMEYER: Thank you again from an industry and participant perspective, the surveys and the piece from FIA are certainly comforting that people have gotten better and better at using the tools and adapting to the tools. And FIA is the perfect organization in my opinion.

Full disclosure, I'm on the Board, I get the privilege of serving with Alicia on the Board of FIA, but FIA does a very good job of canvassing the

industry and getting information back. And these surveys, compared to a few years ago when we continued to have some problems and they've gotten to be much less, but those surveys are certainly encouraging.

A couple of years ago, back when I was working at NFA, we spent a lot of time talking about Reg ATS and trying to get-- Gary's over here hissing at me --

(Laughter.)

MR. HEHMEYER: It got to be very tricky between NFA, CFTC, and the exchanges as to where to draw those boundaries from a legislative standpoint or a rulemaking standpoint as to where to draw those lines of what is and isn't an automated system. A stop for instance, is that an automated system? It gets very tricky to try to come up with language that applies. Well, how broad is it? It can be very difficult to try to impose. And I know that there's some that certainly would like to bring that back up and I'm just offering that that's tough.

One thing that you said, which I think is not -- shouldn't be lost on us, and that is that the participants have asked you for better risk controls.

Right? And so, the prop trading firms, they're -- my biggest fear is that I've missed something and there's some problem right? The FCM's biggest fear is that they'd missed something or one of the firms have missed something. This is the biggest fear that they live with.

Those two groups are very, very competitive and at the exchanges -- I would just offer, and congratulations on getting through that Saudi thing that was a little bit of a hair raising night, but that Sunday night. And I'm sure it was volatility that we haven't seen in a long time on some of your charts, but it was business as usual for you all and thank you for bringing those new tools.

The tools that the exchanges develop, and I certainly appreciate that the exchanges want the firms, the clearing firms and the principal trading firms to take the responsibility for that. I accept it. Bryan Durkin reminds me of it when I have this tussle with him that we are responsible. I get that. Having said all of that, the exchanges are the last place and the better that these tools are, the better

for the whole industry. And so, that's my one comment.

Thank you.

CHAIRMAN GORELICK: Thank you Chris. Superna.

MS. VEDBRAT: So I have, you know, a few questions. You know, you mentioned when we were talking about the -- you know about the controls that you're developing tools for the clearing members to get information from the exchanges or the clearinghouses when there are breaches, you know, set by the clearinghouse itself, you know, on the end users. So my question is like do you share information about an end user portfolio that goes beyond what they're using a particular FCM for?

Because you know, oftentimes you'll use more -- you'll have more than one FCM or more than one clearing member and you know, we just try to keep the information separate.

Of course, the clearinghouse will know how much we are trading, but individual clearing members, we try to keep a book segregated and --

MR. KAPANI: Yes – just to go ahead --

MS. VEDBRAT: I have two more questions, but they’re not all linked together.

MR. KAPANI: So I can answer this one. So essentially, I think you have to look at our world and any, and I'm sure it's true for all exchanges and the trading firms get only the information they are dealing with. Clearing firms only get information about the trading firm for the product they are clearing for that trading firm. And individual participants -- even within the trading firm, there might be cases where they might say that these group of traders cannot see what those other group of traders are seeing.

So all those levels of segregation are part of our standard BAU practice. Information is when you see a Drop Copy you kind of tell us and you also validate with us that you are so and so from here which is trying to connect and this is your connection and we set up an entitlement. We get that entitlement approved internally through a whole set of processes and also with the risk manager at the trading firm that this particular connection which you are

connecting on a private line with this particular connectivity parameters is your connection. And we are willing, we are okay to share this Drop Copy information with you.

So those are the standard protocols we follow. So is portfolio information available? No, it's not available in a general form. It's, it's available for the participant and the clearing member as applicable and their entitlement for the product.

Is that helpful?

MS. VEDBRAT: Yeah, I mean I was just a little concerned if you know, you have multiple FCMs, if there was any sharing of, you know, the portfolio level information, even if it's a breach. Like if you gave a somebody a hundred units and they went, you know, to 101, but it was like 50, 51 with two FCMS I wouldn't necessarily want that --

MR. KAPANI: It would be a major cyber incident. We would be in big trouble if we ever did that.

MS. VEDBRAT: And then, you know, you mentioned development of the self-matching control. I just had a question on as you're developing that, does it take

into account any type of like passive trading or algorithmic trading? Especially like you know, for end-of-day or market-on-close type of -- you know, execution.

MR. KAPANI: So let me tell you how it works and then you can decide whether it fits with a kind of question or kind of things you're worried about.

It takes into account central limit order book matching, which is essentially if there are passive orders sitting on the book and an aggressing order comes in to match with it, we will in real-time look at it and say are these two orders based on the trading firm configuration?

Same user, same account from these group of accounts which the trading firm has told us cannot match with each other. If the answer is they cannot match with either. We prevent it and prevention has a set of things we do there in terms of what actually we do; whether we cancel the aggressing order, whether we cancel the passive order --

MS. VEDBRAT: Okay.

MR. KAPANI: We have a set of rules. So those,

that's what self-match prevention is in our world. End-of-day, somebody’s putting a block position between two people intentionally and giving it to us that we don't look at it as a self-match prevention. This is real-time where the orders that are flowing in because they are running through multiple algorithms or coming through different desks and the trading firm wants to not unintentionally trade these two orders. That's the prevention which we have built.

MS. VEDBRAT: Okay. So you have a control at the trading firm level?

MR. KAPANI: At multiple levels.

MS. VEDBRAT: At multiple levels, okay.

MR. KAPANI: It can be at the account level -- group of accounts level or the trading firm level.

MS. VEDBRAT: Okay. And then, this is my last question. On the Bitcoin futures. Does it use the same default fund for the rest of your futures contracts or does it have its own default fund?

MR. KAPANI: Yeah, so I think it's a little more it's very nuanced and I will probably get it slightly wrong, but I'll try my best. So the way we have it is

our guarantee fund, the way it works is if it is Bitcoin that has been part of the default, there is a initial 35 million just for that. Then we go through the regular risk waterfall.

So Bitcoin has a separate waterfall initial amount, which has been put back in addition to the regular risk waterfall. So I think that’s how it's structured. And the other thing we have structured is there is also a whole insurance side of it where we've got an external insurance for any kind of theft and breach. And I don't know all the nuances of that, but we've got a separate insurance just for those kinds of breaches related to Bitcoin, or virtual currencies.

MS. VEDBRAT: It's just that, you know, if there are, you know, clients who've made a decision that they don't want to have exposure to Bitcoin, just want to make sure that there isn't like an indirect or an unintentional exposure that they may have. It sounds like --

MR. KAPANI: Yeah, point taken. Point taken. We got a lot of feedback when we were launching the product and so we structured the product accordingly.

Thank you.

CHAIRMAN GORELICK: Okay. Thank you very much for those good questions Superna. I think Commissioner Quintenz may have one comment. Oh, we'll give Erik a chance for one last question and then we'll turn to Commissioner Quintenz.

MR. BARRY: Sure. Related to Superna’s first question. Given the give-up nature of the futures markets, particularly asset managers, how does ICE and the FIA best practices consider the fact that I, as the executing firm may be executing throughout the day? How do your margin-based limits think about the likelihood that I'm going to be giving those trades up to another broker where I have no visibility into the established positions there. If they're offsetting, if they're putting a risk on.

How do you guys think about that when it comes to the tools that both the CCP level and the FIA best practice?

MR. KAPANI: Yeah, I think, let me first start with how we think about this. So, obviously it's an evolution in terms of we started with top day, that

margin limits what you are doing today you don't want some -- it's a check where you don't have some runaway set of trades that are occurring that are going to breach margin by a given number. So that's what we started with.

Then we evolved where we let customers put in their start of day positions so that they can say, okay, this is what I'm starting with. That's my baseline include it in your margin control and now you protect against that. Then the third level there, which we have -- which we are moving to, which is essentially incorporating any give ups and the logic or allocation give ups at the backend where it is distributed to a set of funds or to a given asset manager post-trade into this calculation.

The thing we have run into and which is again, based on the information that is provided, we sometimes don't know who to allocate it to the actual block. Many of the clearing firms and the brokers just don't have that information at that point in time or the, it's not in a form that can be consumed when exactly mapped to the a given participant or a given

firm on the frontend. Once that -- and that information flow is improving, but as soon as that improves it will, it'll automatically get incorporated into the regular risk management flow.

That’s a great question.

MS. CRIGHTON: I'll add to that from an FIA perspective. I think, you know, you can think about it on a couple of different fronts. One is certainly the kind of principles that we walked through apply to that. But I think separately there's been work by both FIA and FIA Technology to just sort of start to put some of a more robust framework around thinking about how give ups are done. Right?

We have the give-up agreements. There's been provisions in those agreements in order to be able to set limits. I think as we saw with the initial launch of Bitcoin futures there was sort of a lack of standardization around clearing firms and FCMs communicating that they didn't want to take or clear Bitcoin futures that were traded away.

So it sort of, I think, where the industry has evolved is standardization around setting limits and

communicating those limits, which then I think kind of brings back to the ecosystem more of a sense of responsibility about what is the role of the broker in terms of setting credit limits and what is the role of the FCM in communicating credit appetite or willingness to say this is the amount that I'll clear.

And I think FIA and FIA Technology's really been at kind of the epicenter of driving some of that industry standardization to sort of force that communication. Right? I don't think we can think of it in a world where the executing broker is completely isolated from the FCM and the client's somehow in the middle. Really we need to think about what is the risk management practices at the client, at the broker, and at the FCM. And then from an exchange perspective, how do all those pieces come together? And I think a lot of the work that FIA has done is really bringing those pieces together.

CHAIRMAN GORELICK: Thank you. Commissioner Quintenz.

COMMISSIONER QUINTENZ: Thanks, Richard. I just wanted to make a quick comment that I think sometimes

there can be the perception that if there isn't a new regulation, there isn't any advancement of innovation or the addressing of risk by the marketplace or the private sector. I think these presentations show exactly the opposite that the marketplace, the industry, the participants have been all over these types of risks and for very good reason that there is a very strong business interest and ecosystem interest in addressing these at the exchange level at the clearing member level and at the firm level.

And I would compliment both of you and your organizations for the amount of work that you've done, the amount of activity you've undertaken, and proactivity that you've shown in this area.

And I'm personally very interested in any analysis of the data that FIA has in any refreshing of that, of that data in the future. So thank you both.

CHAIRMAN GORELICK: Okay, thank you. We will take a five minute break and return for the Cybersecurity Subcommittee presentation.

(Recess.)

CHAIRMAN GORELICK: Okay. I would now like to

turn to the final topic on our agenda in which members of our Cybersecurity Subcommittee share their current efforts and work streams going forward. At the end, the committee would like to discuss whether the TAC should vote to recommend the Commission issue a statement of support for the FSSCC cybersecurity profile at the next upcoming TAC meeting.

Our panelists today are Tim McHenry, the vice president of Information Systems at the NFA, Josh Magri, Senior Vice President and Counsel for Regulation and Developing Technology at the Bank Policy Institute, and Jason Harrell, the Executive Director and Head of Business and Government Cybersecurity Partnerships at DTCC.

Tim and Josh will present on the Financial Services Sector Cybersecurity Profile and Jason will present on the current approach to Vendor Risk Management, the challenges of that approach and possible alternatives to consider. I will turn it over to Tim first.

MR. McHENRY: Thank you, Mr. Chairman. So on behalf of me and my working group, a partner Tom Price

from SIFMA, I'd just like to thank Commissioner Quintenz and the TAC for this opportunity to present the Cybersecurity Subcommittee's proposal for having the CFTC issue support for the FSSCC Cybersecurity Profile.

I'd also like to reintroduce Josh Magri, Senior Vice President at the Bank Policy Institute. Josh has been instrumental in the development and the promotion of the profile and if you'll recall he did a comprehensive overview of the profile during the last TAC meeting back in March. During that presentation, he showed how the profile was developed, how it can be used, and he also discussed the growing public support the profile has received; both from firms and from oversight organizations.

So the purpose of our presentation today is to introduce the our proposal, because at the next TAC meeting, like Richard said, we'd like to have the committee vote on whether to recommend that the CFTC join these other oversight organizations and issue a statement of support for the profile. Your materials include a memo that outlines our proposal. We'll go

through that proposal briefly and Josh will also be happy to address any questions or concerns that you may have. He's also doing a presentation to cover the profile as well.

So regulators in the Financial Services Sector have recognized the risks posed by cyber threats and they've been responding with strong risk and principles-based regulation. However, firms are finding that a significant amount their resources are needed to interpret and evaluate these new regulations. Consequently, the fear has been that valuable resources were being shifted more towards the evaluation and interpretation of regulations at the expense of the actual application of security controls.

So members of the FSSCC recognize this issue. And so, in light of growing resource shortages in the information security field, they sought to coordinate an industry-wide effort to create a more organized and consolidated catalog view of various regulatory standards so firms could better survey and address their obligations. They also decided to map this

catalog to the highly regarded NIST Cybersecurity Framework to help firms engage in further risk-based evaluation into remediation using that NIST model.

So over the span of more than I think 50 different working sessions and with the participation of some 150 different financial institutions, the participation of over 300 individual experts and with the leadership of people like Josh, the Cybersecurity Profile was created. And with that, I'd like to turn it over to Josh to talk a little bit about the profile and the process.

MR. MAGRI: Thank you Tim and thank you Commissioners. Thank you CFTC staff and the TAC for inviting me here. Mr. McHenry provided a wonderful overview that I'm just going to really expand upon here. I have a number of slides and if at any point if it's in accordance with your procedure, feel free to interrupt, ask questions. But as Tim mentioned, I'll be willing to take a questions at the end as well.

The first slide that I'm going to show is a slide that you all have seen before. And this is really a

slide that, you know, the saying is, if a picture is worth a thousand words, this is certainly one of them. This is actually worth about 2,300 regulatory questions, provisions, and other related guidance, et cetera. And what this depicts is essentially those provisions being mapped against the NIST Cybersecurity framework.

And we call this the wiring closet because this is what the information security professionals were spending their time doing. They were essentially taking each of the pieces of guidance, the questionnaires, et cetera and trying to map them against their existing programs to see whether or not they fit their current programs, if there were any deficiencies within their programs and whether or not there was any type of overlap amongst the various pieces of regulatory guidance.

So while this is somewhat of a scary graphical depiction and represents the 40 percent of time that information security teams were spending on basically disentangling, there's also a lot of hope here. The hope is that that there was going to be a more optimal

way forward and that there would be the ability for those firms to organize against the NIST Cybersecurity Framework.

So the next slide, I'm going to draw your attention to the right hand piece first of all. That is essentially the last slide, disentangled. It is an architecture that is based on the NIST Cybersecurity Framework as well as IOSCO's piece that came out in 2016 about cyber resilience for financial market infrastructure. And what we did was we took a look at the guidance that had come out and after the mapping, we saw where there was this overlap and the overlap was about 90 percent. And, but we wanted to also see where there, there was opportunities for enhancement, improvement based on what the regulators said.

So we took the NIST five functions of identify, detect, protect, respond, recover and added a piece around governance and dependency management, which is what we found within IOSCO, in which was something that the examiners were appropriately focusing on during the exams.

We extended it to be a little less Socratic than

this to actually be much more assessment-based and diagnostic and scope. So we added a column that is called Diagnostic Statement. And these diagnostic statements are essentially a synthesis of where you might have the nine federal financial services, regulatory agencies saying essentially the same thing, but in different words and putting them in different words.

You know, a good example would be if the nine regulators said you should have a senior information security professional reporting to the Board and then varied up and said, you should have a chief information security officer reporting to the Board. We essentially just took what was the dominant phraseology and said, have a chief information security officer reporting to a Board about X-amount of times per year. And then, we mapped it to those pieces of guidance, those exam questions the regs, et cetera.

Now the left hand side is where I would actually anticipate in quite a few questions from the TAC. In creating the architecture and the underlying

infrastructure. One of the things that we knew that we had to do was essentially scale this thing so that it would work for not only the firms that are quite large and interconnected, but also the 10-person broker-dealer.

And so, the way that that we did that is we started to take a look at some of the guidance pieces that were coming out, as well as some of the old ones that, that you all actually generated post-2001. And we decided to take a look at how a firm might impact the overall economy if it was felled by a cybersecurity attack. And so, then we striated by whether or not a firm would have a global impact, a more regional impact, more of a sector based impact, or a limited impact. And based on how those firms answer a nine question impact assessment, they would then have to answer a series of questions.

So for smaller institutions, it would amount to about 136 diagnostic statements, but that would be something that they would go over with the examiners from each of the agencies to determine if 136 was too few, too many, et cetera. But that was -- that was

how we went about doing it. We were very conscious because we had been asking a lot of the regulatory agencies and oversight agencies not to reinvent the wheel. So we were very careful not to do so as well.

We took a look at designations that were out there such as systemically important financial institutions that were global in scope. We took a look at GLBA and made sure that at the most basic level that impact here for that it correlated directly with the requests out of GLBA. And we filled in really the in-between with things that we were seeing from all of you.

And as Tim mentioned, the way that this was constructed, it really was a cooperative endeavor. We had 150 financial institutions providing input and 300 subject matter experts from them, but we actually had input from the nine federal regulatory agencies as well as the self-regulatory organizations. And that was crucial to this this development.

NIST, in fact, which of course has produced the NIST Cybersecurity Framework. They held an open workshop wherein they invited the regulators and us

and the public to essentially work on this scaling and stratification. And we've worked with NIST quite closely from the beginning of this to its released on October 25th and we'll talk about some of those statements of support. You'll see NIST in there to current day because we plan on keeping this evergreen and making sure that that the versions change with both the regulatory expert expectations but also the threat landscape.

So turning to the documented statements of support since I was here last there are two that are notable. One is actually from a group that you all at the CFTC belong to. It's the International Organization of Security Commissioners. In the June/July timeframe, they completed the Cyber Task Force Report and essentially reading through the report. What was clear is, was a request of the member agencies not to reinvent the wheel as it relates to a cybersecurity assessments.

And they pointed to a number of assessments that already exist, about seven or so in number, but they specifically called out the profile throughout the

document and talked about how comprehensive it was and how it incorporated much of the items including the IOSCO piece from 2016.

The other one that's most recent that's notable, is the Federal Financial Institutions Examination Council, in late August put out a press release based on similar requests that we're making of you all stating that the profile would be acceptable as an assessment approach. And so, on August 28th they said that that firms should be utilizing a standardized assessment approach and named the profile along with three others; their own, the NIST Cybersecurity Framework upon which this is based, as well as what was known as the SANS 20, but is now known as the CIS 20.

One that isn't here because it's not necessarily a statement of support, but the support is certainly implicit, is from the National Association of Insurance Commissioners, which is an organization representative of the State Commissioners. They actually started to map some of their revisions to their IT examination handbook, which is given to the

states to the profile. So with that, we would like to add the CFTC to the list of those that could provide a statement of support. We are expecting more statements, both the domestically within the US, and as well as internationally.

Any questions?

CHAIRMAN GORELICK: Why don't we wait until after Jason's presentation to do questions together. Jason.

MR. HARRELL: Okay. Wonderful. So good afternoon and I want to thank the Committee for the opportunity to present what is a new approach to vendor management and what I would like to call the age of resiliency. I think that resiliency, it's one of those areas that has moved to the forefront as we kind of evolve from cybersecurity and then how do we actually bring systems up and make sure they're functioning to more of a service-based model and how do we actually provide products and services back out to the marketplace in the face of disruptive events.

Vendor management is an area where we have, you know, continued to try to make strides forward as a sector, as supervisors, and that standard setting

bodies in order to improve or enhance the way that firms actually manage the risks associated with their vendors. And in this new age of resiliency when we're looking at the current approaches that we're using as a sector and as supervisors, we had to ask ourselves, you know, is what we've been doing for the last 20 to 25 years in the area of vendor management the way that we should be continuing moving forward in the face of the new threat landscape?

So at the March TAC, we briefly spoke about the number of supervisory documents that were out, there is over 15 supervisory documents that were reviewed and assessed by the subcommittee. In addition to the vendor management life cycle, which is basically the process that firms use in order to manage their vendor risks. Additionally, we requested from the Committee if it was okay for us to look at different approaches to vendor management. And we got that support from this committee. And I thank you for that.

And by allowing for a different approach, we're able to take a revised look at the vendor management process and recommend a direction that we believe will

support a more orderly functioning of the markets and will support the resiliency efforts that firms' market participants, market operators, standard setting bodies, and the like that are currently underway.

So just as a bit of background, we already understand that as the financial services sector, we've seen a marked increase in the frequency and the scale of cyber attacks. This is largely due to the skill and determination of many of the threat actors that have focused on extracting funds or information from the sector. This risk has been made systemic due to the global interconnectedness of the marketplace as well as the complexity of the supply chain used to deliver products and services back out to the market.

A new entrant into the financial markets continued to cause disruption to the current way that firms and consumers engage in this marketplace. And the supervisory regime is continuing to mature in this space. From market resiliency, it continues to be a priority for many jurisdictions. And to achieve this resiliency, we understand that it takes more than system availability to provide a product or service

and requires an understanding of the entire supply chain needed to deliver that product and each supplier needs to have a certain amount of resiliency built into their operations for the sector to have a reasonable amount of assurance that there's a continuation in the services to the marketplace.

When reviewing the current approach that market participants and operators and supervisors have adopted to manage these risks, we've noted that in the process it may not be optimally designed to manage the risks that firms face from their vendors and achieve the level of resiliency that is -- that we face in today's threat landscape. As a result, we are proposing a new approach that may create a more equitable risk balance between financial institutions and the third-party vendors.

So as firms continue to partner with new and innovative solutions providers, I expand their delivery methods of existing products and services and develop new solutions for consumers the suppliers use to complete these activities, increase the surface area available for threat actors to negatively impact

this marketplace. A number of the new entrants that outside the regulatory perimeter while providing critical services to firms that provide critical services back out to the marketplace. Because of this threat, it's important that market participants and operators have sufficient visibility into the operations of the supply chain to provide a desired level of resiliency.

So when I talk about resiliency, because I always try to make sure that we're all on the same page with results to terms, is I'm speaking on the practices and disciplines that enable firms to provide products and services to the marketplace in face of disruptive events, regardless of the nature and origin of those events, by anticipating, preventing, recovering from and responding to such events.

Over the last 18 months, resiliency activities have ramped up from market participants, operators, supervisors, standard setting bodies and trade associations to improve resiliency across the sector. Several supervisors have also released consultative documents on their position on resiliency to express

back out to participants and operators their views and thoughts on this topic.

In addition, a working groups have been established to identify and develop ways to help the sector improve resiliency and to support the sector resiliency efforts. Through the course of these efforts, it has been uniformly agreed that a service-based approach to resiliency must be taken in order to raise the level of assurance that a sector can provide a minimum viable product back out to the marketplace in times of extreme market stress. This includes not only the firms but the supply chains used to deliver these services.

So that kind of outlines where we are today. What I would like to shift our focus to is the current way that firms and supervisors are actually approaching the vendor management challenge. With respect to the supervisors and regulators, supervisory documents have provided firms with a range of guidance requirements from general vendor management expectations to more detailed vendor management rulemaking for vendors that are deemed to be critical.

In most cases current rulemaking doesn't consistently provide guidance across all the different areas, but usually provides guidance in specific areas within the vendor management life cycle. From a firm perspective, considerable bandwidth is really put into three of these areas. And that's on due diligence and third-party selection, contract negotiation, and ongoing monitoring.

The way that firms approach this is they stipulate numerous security requirements in their contracts in order to address the risk that may arise from using a vendor. In addition to these contractual terms, firms also use questionnaires in order to understand the types of controls that a vendor may have in place. These are normally comprised of hundreds of questions. Many of them are yes or no questions. And even more are open to interpretation by the individual or individuals who are completing the form.

During the course of the contract, and if it's agreed to within the contractual terms, the same questionnaires are resubmitted to the vendor to answer

again and verify that the controls that were, are still in place, that were in place at the beginning of the contract. Additionally, several vendor or client meetings may also be involved to get a greater understanding of the control of information.

What this leads to is a very process intensive means of control verification for the firm and for the vendor, it's at least an order of magnitude higher depending on the number of firms for which it provides a service.

So what are the current challenges that we have? I would say we really have four challenges that arise from the current method of vendor management. The first one and probably the largest challenge is just the risk visibility and questionnaire fatigue. Since questionnaires are used to gather information on the controls structure in place with the vendor and these questionnaires are of a different variation depending on the firm and they consist of hundreds of questions, it becomes very onerous for vendors to complete. More importantly these questions actually provide a limited understanding of the true business risks that a firm

faces when using a vendor. And it does little to validate the vendor's ability to be resilient in times of extreme market stress.

Again, for the vendor they're required to, you know, complete hundreds of questions for all of the different firms that they support.

The second one is the compliance to multiple foreign policies, the standards, as part of the contractual agreement process many of the firms request that the vendor adhere to their policies and standards and It's easy to see that once you get a number of firms and you're trying to adhere to each of their policies and standards, it could be different controls structures that we use at firms that we're trying to then put onto the vendor, and it just leads to a number of requirements for the vendor that are difficult, if not impossible for that vendor to accommodate.

Intellectual property protection. So vendors are also hesitant to disclose the technical details of the - - and design vulnerabilities within their applications or services, as this may compromise the

application or service if it's accidentally leaked out to the public. In addition, vendors will not provide access to the source code in order for firms to actually understand the risks associated with the product.

And then the last one is a contractual leverage. Since there's a difference between small and large vendors and small and large firms, it leads to an inequitable distribution of the risk, which I will detail on the next slide.

So I'll start, you know, basically at the top left corner on the out of out of box security. So small financial firm, large vendor. The small financial firms have fewer resources to manage the complex vendor relationships. When dealing with large vendors, they're normally forced to agree to the current security solutions that is offered by the vendor. Additionally, the level of oversight that is able to be negotiated by the firm is less than -- based on the just the cost basis of the contract and therefore they have little room to influence or make changes to the contract to get the additional

visibility that they would like.

If we go to the small financial firms, small vendor, which is in the bottom left hand corner, the vendor may have limited resources to provide all of the security offerings that may be needed and the financial firm then also has limited influence based on the contract size to make the changes.

If we go back up to the top right hand corner where we have complex relationships with limited effectiveness, again, the complex contractual relationships based on what was conceded to or agreed to in the contract is difficult-to-impossible for the vendors to meet all the contractual obligations. There's a limited ability to get right to audit clauses as this could lead to a never ending cycle of audits from the firms that the vendor is trying to support which could ultimately lead in conflicting guidance on how to address the risks.

And then, if you have a small vendor and a large firm, the vendor basically tries to agree to all of the customized solutions for the financial firm just because of the size of the contract, which leads to

higher service costs as they tried to build niche solutions for the different large financial firms.

So given this, the challenges from the prior slide and the contractual challenges here, the current vendor risk management model may not be optimally designed to support the resiliency required to provide a minimum viable product or service to the marketplace. As a subcommittee, we believe that we must consider a different vendor management approach that is an equitable risk balance between the financial institution and the third-party provider in order to deliver the level of resiliency in this new threat landscape.

So from a potential new approach, you know, developing an industry certification that is dependent on the size of the vendor and the risk posed by the vendor product or service to the entity and to the sector, the industry will realize several benefits over the current method utilized to identify vendor risks. The first one is reduce questionnaire fatigue for firms and vendors. Since firms will know that the vendor has been certified against an agreed set of

resiliency and security requirements based on the vendor service provided to the marketplace, this certification will need to then be reviewed on a periodic basis as determined by the risk level. This will reduce the need for the questionnaires between marketplace, market participants, and vendors since the resiliency standard will have been set and verified through the certification process.

Vendors will bear additional accountability for maintaining their certification with the understanding that their risk level may change based on certain risk factors. For example, increased market penetration or market share or concentration risks that may exist when you have a limited amount of vendors that provide a product or service to the firms.

The second one is common agrees in the industry certification harmonizes the requirements of multiple firms, again, by establishing an industry certification, the number of disparate from policies and standards that are contained within the contractual language between firms and vendors can be coordinated while achieving the industry's risk

management goals. The third thing is it simplifies the contract language relative to cybersecurity. Firms can require that vendors maintain their certification as part of the contract, contractual agreement. And this could limit the length of security addendums that are appended to many of the vendor contracts. And then, last but not least, there's a greater level of resiliency assurance.

In this model, the smaller firms will also have the ability to gain an understanding of the resiliency of a vendor in a more comprehensive way than in the prior model, because the questions that they would like to have answered will be addressed through the certification process and then the firms can have better assurance that the controls and the level of resiliency is in place.

So while other approaches have been considered, this was actually represents the best approach for this challenge. We did look at a couple of other options for doing vendor management, oversight and implementation. One of those was around, you know, providing direct supervisory oversight. But while

this -- will it have a benefit for the critical functions, it still doesn't address the questionnaire fatigue that will still occur. It doesn't limit the compliance requirements that firms will put onto the vendors. And it still doesn't address the contractual inequity between the firms and vendors that were described before.

The other challenges that as a subcommittee, we're not clear on the number of critical service providers that firms would have in this space. So without that information or knowledge it's hard to understand whether a direct supervisory approach would add any substantial benefit or would be feasible for the number of vendors that could then be pulled into that space.

And then the last one was, we really looked at around what if we combine industry certification and direct supervisory oversight. But in that space you really still get -- you get all the benefits of the industry certification, but you don't necessarily get additional benefits from the direct supervisory oversight.

So again, given that you know, we looked at all three of these and we decided that these new approaches for the industry certification best served the sector we want to provide some visibility into that new approach and answer questions around that.

Thank you for thank you to the Committee and I'll pass the floor back.

CHAIRMAN GORELICK: Thank you very much. Those were both very informative presentations. I'll start off with my own question and then I'll turn it over to the floor.

So this is for Josh and for Tim. So I understand that you are mid-term goal here would be to get an endorsement from the CFTC of this approach after a vote by the Technology Advisory Committee to recommend that to the Commission. What is your longer term goal as it relates to the CFTC? Would it be for new rules and regulations that somehow integrate this process and framework or changes to the auditing functions? You know, what would you like the Commission to do longer term beyond justice endorsement?

MR. MAGRI: Sure. So I know that the term

"endorsement" carries a lot of weight. What we've been asking for agencies to do is supply a statement of support.

So that would be on the shorter term, the longer term, yes, we would, we would appreciate if agencies such as the CFTC take a look at the profile, its organizational structure, and if they're thinking about new regulations, new guidance, et cetera, that they do really one of two things. The first would be something similar to what the National Association of Insurance Commissioners did, which is when they were updating their IT examination handbook, they did a straw man mapping of those amendments to the profile and put it out for public review and comment.

Alternatively, one of the things that we would appreciate is really just having I guess a conversation or some type of public comment period where when you, you put it out, you put some level of reference to the profile and then we could work with you through the traditional processes to developing a mapping of those regulations going forward.

CHAIRMAN GORELICK: Okay, thank you. Brad.

MR. LEVY: Thank you. Jason, so your presentation was great. Thank you. It's about onboarding and maintenance. Have you thought of, and in terms of the actual event management, where something happens, like a POODLE, a malware moment where you're looking to get to all of your relationships, third-parties upstream and down, who am I dependent on? Who's dependent on me? And a lot of these systems are -- some are vendor management systems. Some were more policy and then, some were more event management. People are thinking it's more of a continuum and can there be one system that kind of handles all of that, including the in the moment kind of back and forth that will go on when you're actually trying to figure out “where am I exposed to” as the event is unfolding.

MR. HARRELL: So what I'll say is that, you know, one of the things that we're looking at from a resiliency standpoint is, you know, number one, what are the services that firms provide that are critical to the market functioning. So, you know, sitting down, for example, for DTCC we do clearing and

settlement and those are critical to the folks in the marketplace.

In order to provide clearing and settlement, we also rely on a number of third-party firms in order to provide clearing and settlement back out. So the requirement in the past has been “Well, can you as DTCC have your systems up within two hours?”

And now we are looking at it from a sector and you know, from supervisors to the sector of you know, we understand that having systems up in two hours may not -- still may not provide that product or service back out to the marketplace because you know, one, everybody still needs to have the same view of the marketplace that they're operating in. And number two, is you still have a number of providers that you -- in order to provide that service back out, need to be functioning and have resiliency built in as well.

So, you know, in the past when we were looking, you know, just at the firm themselves, we go -- okay you know, if we have a system and we can get it up in two hours, you know, you could check the box, you can continue to move forward. Now with the new

expectation of can you provide that product and service we are looking at, we have to take a look at our vendors a little bit more closely in order to be able to answer that question.

The challenge that we have now is, is it enough for us to use questionnaires and, you know, basically, you know the self-attestations that we get from the vendor in order to have reasonable assurance or is that bar going to change and say no, more needs to be done in order to understand that there's true resiliency with those vendors to provide that product or service out, so that we can have orderly a functioning in markets.

And I think that, you know, for the last 15, 20 years we've been using these questionnaire-based approaches and maybe the threat landscape has changed to enough now where that is no longer enough to provide a reasonable assurance that we can provide a product and service to the marketplace and we need to do something a little bit more to drive that assurance. So then the question is what does that look like?

MR. MAGRI: I was wondering if I might return to your question about request. The one thing that I neglected to mention, I think that you hit upon, was a examiner training. That is something that we've requested of the other agencies and the other agencies have said yes to. Because really we want to make sure that the profile as an assessment works for not only the firms that use it in terms of simplification, but for the examiners as well. And we found that having an ability to talk to the examiners and provide some level of training essentially it helps, you know, in the field.

CHAIRMAN GORELICK: Okay, thank you. Gary.

MR. DeWAAL: So I found this very, very interesting as someone who has often negotiated in my life with vendors on requirements and things like that. And I agree, it's -- there's a definitely an unequal bargaining position when you're either dealing with somebody who's new in the industry and really doesn't have the resources and is very afraid to commit to anything versus a monopolistic service provider spectrum where basically you've got to take

it or leave it. So you know, that those, those are issues and I'm not sure necessarily that those are solved by a certification accreditation system.

Particularly if the goal is to reduce the length of legal documents. I can imagine a scenario where you know, a third party is now participating in this certification or the accreditation effectively you're opening up another party for potential liability in the claim. And I'm curious who would be willing to step up to that.

And I'm also concerned as you just said about the qualifications of the folks who might be doing the certification accreditation. You know, how can industry participants be satisfied that the certification or accreditation means anything.

And there’s sort of a question in there, but I guess also my final question is I understand questionnaire fatigue, I absolutely understand that, but is the answer maybe not more standardized disclosure by vendors themselves as how do they deal with certain, and I understand it's based on their own bias or their own, you know, their own view, beliefs.

It's out there. It's a standard. And if they commit to that publicly, certainly from a liability perspective, that's not a bad thing if something goes wrong down the line.

MR. HARRELL: So I'll answer the last question first.

MR. DeWAAL: That’s the new trend today, the second question is answered first.

(Laughter.)

MR. HARRELL: So again, I think it depends on the level of assurance that we need to provide as a sector when dealing with resiliency and, you know, and I'll just lend my own personal opinion here is that we're talking about, you know, especially around critical services being able to be provide it back out to the marketplace. You know, my personal opinion and my personal concern is that these are things that we considered material for the orderly functioning of the markets.

So I don't want to really get to a point where I'm working on legal, you know, legal contracts around, “Well, you're supposed to do this, you're

supposed to do that." It gets real dicey. So I don't know if just relying on the vendor to provide a statement that they're doing the things that they need for resiliency will be sufficient with what is the table stakes for that.

You know, again, this is something that we're now, you know, trying to think through. So again, understanding or agreeing -- having some level of agreement of what is reasonable assurance in the case of maintaining an orderly market.

The answer - - the next question around are we introducing more liability and legal implications by having an accreditation model is, I mean, this is why – you know I think, one of the challenges I have for this model is it's going to require a high amount of coordination between the market participants, vendors, standard setting bodies because we also need to say, you know, what does resiliency actually really mean?

So before we can even start talking about all the legal aspects of it, you know, what is going to be required from not only firms but from their suppliers to say that they have adequate resiliency? And then

once that is established, you know, how does that then translate into what we need for vendors? And I think we're still working through that.

There's been a number of consultation papers on it. I believe that this -- later this month, the UK Supervisors will be putting forth an additional consultation document to follow up their 2018 consultation document on resiliency. So, you know, I think we're getting closer to a solution there. I just, you know, again, believe that we need to have a stronger model to assure the resiliency to the marketplace than what may be in place right now.

CHAIRMAN GORELICK: Okay are there any more questions from the committee at this point?

(No response.)

CHAIRMAN GORELICK: Okay. So, that was great. Thank you all for your comments today. We've had a lot of good updates and feedback from our subcommittees. We look forward to the ongoing work of our subcommittees and efforts of the broader Technology Advisory Committee. I would like to now turn back to Commissioner Quintenz so that he can give

his closing remarks.

COMMISSIONER QUINTENZ: Thank you. Nothing formal. Just to reiterate my sincere thanks for everyone's hard work. I mean, meetings like this, especially with such robust presentations require, you know, a constant commitment of time and energy and thought and ideas and preparation and then to come here and travel, you know, and reserve your schedules. It's very meaningful for me. I receive a great deal of benefit from these conversations from all the conversations we have. So just my, my sincere thanks for being here today and participating so robustly.

MS. TENTE: All right. With that, thank you everyone for attending. The meeting is now adjourned.

(Whereupon, at 3:28 p.m., the Commodity Futures Trading Commission Technical Advisory Committee meeting was adjourned.)