MINUTES OF THE MEETING OF THE
U.S. COMMODITY FUTURES TRADING COMMISSION'S
TECHNOLOGY ADVISORY COMMITTEE
October 3, 2019

The Technology Advisory Committee (TAC or Committee) convened for a public meeting on Thursday, October 3, 2019, at 10:00 a.m., at the U.S. Commodity Futures Trading Commission's (CFTC or Commission) Headquarters Conference Center, located at Three Lafayette Centre, 1155 21st Street, NW, Washington, DC. The meeting consisted of four panels. In Panel I, the TAC Virtual Currencies Subcommittee reviewed the different natures and characteristics of stablecoins and the potential implications for regulation. A second presentation discussed cryptocurrency custodial relationships and custodial options. In Panel II, the TAC Distributed Ledger Technology and Market Infrastructure Subcommittee covered data privacy, and the applications of distributed ledger technology (DLT) in derivatives markets for custody and collateral management. In Panel III, the TAC Automated and Modern Trading Markets Subcommittee discussed best practices for managing risks associated with automated trading systems and related market implications, highlighting best practices of the Futures Industry Association (FIA) and risk controls currently employed on the Intercontinental Exchange (ICE) trading platform. In Panel IV, the TAC Cybersecurity Subcommittee discussed the Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile. A second presentation covered the current approach to vendor risk management, the challenges of that approach, and possible alternatives.

TAC Members in Attendance
Richard Gorelick, TAC Chair, Head of Market Structure, DRW Holdings LLC
Erik Barry, Head of Client Platform for Prime Derivative Services, Credit Suisse
Christopher Chattaway, Managing Director, Goldman Sachs
Thomas Chippas, Chief Executive Officer, ErisX
Charley Cooper, Managing Director, R3
Gary DeWaal, Special Counsel, Katten Muchin Rosenman LLP
Christopher Hehmeyer, Managing Member, Hehmeyer Trading and Investments
Mayur Kapani, Chief Technology Officer, ICE
Derek Josef Kleinbauer, Vice President, Bloomberg SEF LLC, and Global Head of Rates and Equities Electronic Trading, Bloomberg L.P., Bloomberg
Brian Knight, Senior Research Fellow, GMU Mercatus Center, Special Government Employee (SGE) for CFTC
Bradford Levy, Senior Vice President, Global Head of Loans and Chief Executive Officer, MarkitServ, IHS Markit
John Lothian, President and Chief Executive Officer, Jonathan J. Lothian Co.
Timothy McHenry, Vice President, Information Systems, NFA
Lee Olesky, Cofounder and Chief Executive Officer, Tradeweb
Alexander Stein, Managing Director, Two Sigma Investments, LP
Larry Tabb, Founder and Research Chairman, TABB Group
Supurna VedBrat, Global Head of Trading, BlackRock
Yesha Yadav, Professor of Law, Vanderbilt University, Special Government Employee (SGE) for CFTC

Speakers in Attendance

Gary DeWaal, Member and Co-Chair, TAC Virtual Currencies Subcommittee, Special Counsel, Chair, Financial Markets and Regulatory, Katten Muchin Rosenman LLP (Panel I, first presentation)

Lee Schneider, General Counsel, block.one (Panel I, first presentation)

Chris Brummer, Special Government Employee Member, TAC Virtual Currencies Subcommittee Professor and Director, Institute of International Economic Law, Georgetown University Law Center (Panel I, second presentation)

Thomas Chippas, Chief Executive Officer, ErisX (Panel I, second presentation)

Bradford Levy, Member and Co-Chair, TAC Distributed Ledger Technology and Market Infrastructure Subcommittee, CEO MarkitServ, IHS Markit (Panel II)

Shawnna Hoffman-Childress, Member and Co-Chair, TAC Distributed Ledger Technology and Market Infrastructure Subcommittee, IBM Global Cognitive Legal Leader (Panel II)

Yesha Yadav, Special Government Employee Member, TAC Virtual Currencies Subcommittee, Professor of Law, Vanderbilt Law School (Panel II and Panel III)

Alicia Crighton, Managing Director, Goldman Sachs (Panel III)

Mayur Kapani, TAC Member, Chief Technology Officer, ICE (Panel III)

Ed Prosser, Member, TAC Automated and Modern Trading Markets Subcommittee, Senior Vice President, The Scoular Company (Panel III)

Tim McHenry, Vice President, Information Systems, NFA (Panel IV, first presentation)

Josh Magri, Senior Vice President and Counsel for Regulation & Developing Technology, Bank Policy Institute (Panel IV, first presentation)

Jason Harrell, Member, TAC Cybersecurity Subcommittee, Executive Director and Head of Business and Government, Cybersecurity Partnerships, DTCC (Panel IV, second presentation)

CFTC Commissioners and Staff in Attendance

Brian D. Quintenz, Commissioner and TAC Sponsor

Heath P. Tarbert, Chairman

Rostin Behnam, Commissioner

Dan Berkovitz, Commissioner

Dawn D. Stump, Commissioner

Meghan Tente, TAC Designated Federal Officer (DFO), Special Counsel, Division of Market Oversight

I. Opening Remarks

Ms. Tente called the meeting to order. Commissioner Quintenz began the meeting by welcoming Chairman Tarbert to his first TAC meeting and thanking Ms. Tente for her diligence. Commissioner Quintenz then gave an overview of the upcoming presentations. With regard to stablecoins, he noted that it is important for policymakers to approach any stablecoin consistently with products that have similar characteristics, mechanics, and structure. With regard to crypto custody, Commissioner Quintenz remarked that the protection of private keys by crypto-trading platforms, trust companies, and clearinghouses is an evolving landscape of best practices which has quickly become very robust. With regard to DLT, he stated that DLT holds great promise to safeguard individuals' privacy, promote data integrity and ensure

confidentiality. Commissioner Quintenz commented that, as the technology matures, DLT may be able to help firms demonstrate compliance with CFTC record retention requirements. He suggested that if the agency were ever able to verify over the blockchain that certain records exist within a firm and are being maintained appropriately, that could significantly enhance customer protection and promote regulatory compliance while not requiring enormous regulatory resources or exposing sensitive data to cyber risk through electronic transfers. With regard to automated and algorithmic trading, Commissioner Quintenz noted that many of the risks are being addressed through market incentives, but to the extent there are gaps, his hope is that the subcommittee can begin a conversation about the best way to solve them. With regard to the Financial Services Sector Cybersecurity Profile, he stated that the Cybersecurity Subcommittee would like to discuss with the full Committee whether the TAC should recommend that the Commission issue a statement of support for the profile at the next TAC meeting.

In his opening remarks, Chairman Tarbert stated that the TAC has a vital role to play as the CFTC regulates markets that are at the cutting edge of technological innovation, but the agency does not always have the technological expertise that market participants have. The CFTC can keep pace with market developments only through dialogue with people active in those markets and driving those developments. He stated that the CFTC's job is to ensure its rules protect market integrity while fostering innovation and the best way to strike a balance between innovation and market integrity is through a principles-based approach that allows flexibility but maintains fundamental regulatory mandates.

Commissioner Behnam gave special thanks to Commissioner Quintenz, Ms. Tente and Chairman Gorelick for their leadership on the meeting and stated that he looked forward to the findings. Commissioner Stump thanked everyone who worked to pull the meeting together.

Commissioner Berkovitz stated that infrastructure technology can be used to make regulatory compliance more efficient. He believes that financial technology (fintech) solutions that digitize and automate swap transactions and life cycle events will lead to compliance that is more complete and cost-effective. Commissioner Berkovitz said the benefits of automation are realized when repetitive processes are standardized, digitized, and automated. He noted that consistency will reduce errors and human input, improving the level of compliance over millions of swaps, and savings can also be expected. Commissioner Berkovitz said the CFTC should play a role in helping fintech providers build automated solutions that are effective in fulfilling regulatory requirements, and the CFTC should be mindful of the role of technology in compliance in its approach to regulation.

II. Panel I: Virtual Currencies Subcommittee Presentations

Chairman Gorelick introduced Mr. DeWaal and Mr. Schneider, who discussed the varying natures and characteristics of stablecoins and potential implications for regulation. Mr. DeWaal stated that stablecoins are not just crypto assets that endeavor to maintain a stable value against a basket or individual assets, they endeavor to maintain a stable value against a target referent asset, which can be tangible or intangible. The manner in which stablecoins are

structured can be critical in determining how and which regulations apply, but even after analysis their regulation can be unclear.

Mr. Schneider explained that stablecoins are digital representations of value and the means of achieving stability can be quite varied. He emphasized the importance of focusing on the functions and features of the stablecoin or any other digital asset. Mr. Schneider stated that stable coins are often designed to be stable against the value of the underlying asset or referent asset, which can be a physical asset like gold or intangible assets like dollars or securities. He said that intangible assets are really human ideas or concepts that we give a legal wrapper to in order to consider them to be assets, and stablecoins are providing a digital wrapper around that legal wrapper to know what the referent asset is. Mr. Schneider explained that human beings have used paper stock certificates to represent shares of stock and dollar bills to represent U.S. fiat currency, and a digital representation of those things is not designed to change the character of them. Mr. Schneider said there has long been a U.S. dollar stablecoin, and it is called a bank deposit account. It is a digital representation where one can access one's account on an app, and regularly transact business through the app in U.S. dollars, none of which is physical currency at all. He noted that people already live in this digital world, and those people creating stablecoins are trying to mimic a lot of the ideas already being implemented, using the power of blockchain and encryption to make them a more transparent, auditable, and safer.

Mr. DeWaal stated that the legal analysis of the regulation of stablecoins is fascinating. He agreed with Mr. Schneider that stablecoins are simply another electronic manifestation of something. He noted that people have long used gold warehouse receipts. Stablecoins should not be treated differently simply because they are a form of virtual asset. That is why it is important to look into the different types of stablecoins, which are based on a continuum of referent assets. For example, he said stablecoins can be based on a single asset, such as the U.S. dollar, which arguably would not be a security under the traditional Howey Test since no manager is involved. In contrast, stablecoins backed by multiple instruments controlled by a manager might be considered a security based on the Howey Test. Mr. DeWaal also discussed the application of the Reves case to stablecoins.

Mr. DeWaal noted that other regulations could come into play, both in the U.S. and other countries. For example, the issuer of a stablecoin or virtual currency could fall under state money transmission regimes. He explained that the issuer could be deemed a payment issuer, the coin itself could be considered a payment instrument, and the transactions on an exchange could also fall within the money transmission regime. Mr. DeWaal stated that at the Federal level, Financial Crimes Enforcement Network (FinCEN), the Bank Secrecy Act, and anti-money laundering laws could come into play. He also stated that The Office of the Comptroller of the Currency (OCC) recently tried to develop a Fintech licensing authority which is being challenged by the Department of Financial Services in New York and other state regulators. He fears that regulators are fighting over turf.

Mr. DeWaal said one could argue that the definition of a "swap" under the Commodity Exchange Act is so broad that a stablecoin could fall within the definition, although he does not think that is the right outcome. He stated that stablecoins represent a continuum that are objects based on some referent, which could be a tangible asset, sneakers, something more intangible,

or an algorithmic device that maintains stability through the process of the algorithm. Mr. DeWaal said one stablecoin was withdrawn even though it achieved approximately $133 million in private equity financing because their method of algorithm was likely to be deemed a security or investment contract by the U.S. Securities and Exchange Commission (SEC). He stated that regulators around the world are formally studying this, partly because of the proposed introduction of Facebook Libra. Mr. DeWaal noted that the Swiss Financial Market Supervisory Authority (FINMA) published guidance on stablecoins based on the proposition that products posing the same risks should be subject to the same rules. Libra would be based on a basket of underlying assets, fiat currency, some government instruments, with details to be fleshed out, and overseen by the Libra Association. Preliminarily, FINMA said that Libra would fall under their financial infrastructure guidance and would require a payment instrument license and would be subject to AML requirements. FINMA also said that because Libra would likely increase risk to the payment system, it should be subject to corresponding requirements. Mr. DeWaal believes that would possibly include capital requirements to address credit, market and operational risk, and risk concentration and the management of Libra reserve. FINMA stated that the risk of the reserve must be borne entirely by the Libra Association, not holders, with details to come upon filing a formal application.

In Mr. DeWaal's view, stablecoins have great potential to expand the usage of blockchain technology. If there was the ability to have a comprehensive blockchain-based system for swaps, it could have powerful implications for reporting because everything is all happening on one system. He stated that stablecoins have the potential to help transactions internationally but the regulatory environment today is inconsistent.

Mr. DeWaal noted that there are initiatives by corporations to have privately developed products like stablecoin (e.g., a JPM coin), on a private permission blockchain and not in the general public. This should raise entirely different issues. He stated that the SEC recently issued a no-action letter to Turnkey Jet, a chartered air company that wanted a private type of stablecoin, and took the position it was not a security. Mr. DeWaal believes we are a long way away from regulatory certainty, and fears that there is a certain amount of turf fighting. Libra also raises privacy concerns, banking concerns, and central banking concerns (i.e., does it undercut the central banks). He stated that a lot of these issues merely amplify existing difficulties under current regulations.

Mr. Schneider then walked through a slide presentation on various stablecoins, including Tether, TrueUSD, Turnkey Jet, Inc., Libra, Paxos Gold, Basis, Maker/Dao, JPM Coin, and Utility Settlement Coin. He stated that in terms of regulation, it is important to look at not only the issuer, but other parties that are involved. He also noted that good quality disclosure is important for purchasers to know what they are purchasing.

Following the presentations, Chairman Gorelick asked whether the panelists had advice for the CFTC or other policy makers about how to clear up some of the ambiguity. Mr. DeWaal responded that absent something clearly being a security, if someone commits fraud, he was of the opinion that the CFTC would likely have jurisdiction and would retain antifraud authority and, to the extent there is leverage, the participants may need to transact through a futures commission merchant and/or a licensed exchange. So the analysis for the CFTC for a

stablecoin is not necessarily different than for other virtual currencies. But to the extent that the stablecoin is stabilized through algorithms, it gets trickier. He noted that the SEC settled an important case with EtherDelta that effectively said that if there is a requirement that something be traded on an exchange, and the exchange is algorithmic, someone has to be responsible if there is a violation. But he does not necessarily believe that the CFTC swap definition should capture these products even though the plain language arguably captures many stablecoins. The international regulators need to address these issues.

Mr. Schneider stated that lawyers and regulators need to go back to existing principles and existing instruments and treat similar products similarly, and not try to create new categories just because blockchain or encryption technology is involved as opposed to some other type of database technology. The use of stablecoins as a payment tool was also discussed. With regard to the use of blockchain to help with regulatory compliance, Mr. Schneider recommended a paper from the Bank of International Settlements (BIS) about embedded supervision and how regulators and financial services supervisors can use blockchain to further their mission. The panelists also discussed the importance of disclosure for stablecoins with both underlying volatile assets or pegged with dollars, particularly with respect to retail investors who may be prone to panic. Mr. DeWaal stated that disclosure is important for stablecoins that achieve price stability through algorithmic mechanisms as people need to understand how that works.

Next, Chairman Gorelick introduced Professor Brummer and Mr. Chippas who gave a presentation on cryptocurrency custodial relationships and custodial options. Professor Brummer explained that custodying of crypto-assets is foundational to market-making, but because cryptocurrencies are essentially digital bearer instruments, there are unique cybersecurity and governance challenges. While custodial relationships vary, there are three basic models: (1) non-custodial wallets (self-custody), which risks exposing customers as the "weakest link" in their own cybersecurity and stymies liquidity but also enables a decentralized architecture with lower paydays for cyber criminals; (2) exchange-based wallets, which can offer greater cybersecurity but are an attractive "honeypot" for criminals and present dangers such as commingling of customer assets, front running, or market manipulation; and (3) third party (non-exchange) custodians, which can provide better cybersecurity than retail holders and alleviate risks of exchange-based wallets where custodians are separately regulated affiliated entities, but still pose liquidity challenges and monitoring challenges.

Mr. Chippas added that technology regarding the custody of digital assets is ever-changing and evolving rapidly. He stressed the importance for the Commission to maintain focus on the application of principles in this area because it would be virtually impossible to stay up with the changes in technology and the evolving operating models, specific to digital asset custody.

Professor Brummer noted that there are a wide variety of potential custodians, including banks and trust companies, broker-dealers, investment advisers/investment vehicles, futures commission merchants, derivatives clearing organizations, and foreign depositories. However, to date few large players have entered the digital asset custody space, possibly due to the inherent riskiness of assets, lack of familiarity with digital assets, questionable robustness of

cybersecurity/technology, and regulatory compliance and litigation risk. Mr. Chippas said that most institutional players are lagging in their understanding, and the risks in this area are outsized compared to other asset businesses they engage in.

Professor Brummer explained that when custodians are in possession of cryptocurrencies when a fork arises, a number of questions arise, including whether a custodian is required to return to the account holder the forked cryptocurrency along with the original cryptocurrency and the speed with which new forked cryptocurrencies must be delivered to the account holder. Mr. Chippas added that the anticipation of all outcomes in forking is impossible, so typically what you see are disclosure of forking policies, so that consumers can determine whether the forking policy is appropriate for the assets they hold.

Professor Brummer stated that a disclosure regime for custodians is needed, and that it should cover cybersecurity practices and limitations, operational risks, conflicts of interest, balance sheet and capitalization, forking practices, and insurance coverage.

Following the presentations, Chairman Gorelick opened the floor to questions or comments from the TAC members. Ms. Yadav asked why any credible providers would want to get in this game, and whether costs would be passed on to retail consumers who would then prefer self-custody, with diminishing liquidity as a result. Mr. Chippas said that most retail customers say "not your keys, not your coin," so many retail customers use self-custody. It will be interesting to see if this trend continues as new customers enter the digital asset space. He noted that a multitude of providers offer high quality solutions, and it is likely that costs will come down as there are new entrants. Mr. Tabb asked about lending and margin, and Mr. Chippas responded that the market has largely addressed it. To Mr. McHenry's question about verification of ownership, Mr. Chippas replied that there are various verification solutions in use by custodians. Mr. Hehmeyer asked why one of the slides mentioned lack of liquidity as an issue, when there seems to be a lot of liquidity offered to customers. Professor Brummer noted that the slide on custodial infrastructures that compares hot wallets (which are connected to the internet) to cold wallets (which are offline) is focused on retail customers. In the case of cold wallets, it can be difficult to access private keys quickly and this can result in illiquidity, which would not be a problem in the case of institutional customers.

[Break]

III. Panel II: Distributed Ledger Technology and Market Infrastructure Subcommittee Presentation

After the break, Chairman Gorelick introduced the members of the Distributed Ledger Technology and Market Infrastructure Subcommittee, who gave a presentation on data privacy and the applications of DLT in derivatives markets for custody and collateral management. Mr. Levy summarized the work of the DLT subcommittee to date. He noted that DLT has application beyond virtual currencies, and that traditional finance is becoming active in adopting DLT.

Ms. Yadav stated that the subcommittee has been excited about exploring the possibility of DLT as a technology that can help safeguard the privacy of users and maintain the confidentiality of financial markets transactions. Markets have become more electronic, and the explosion in digital data creates enormous technological and logistical pressure on providers of market infrastructure and regulators to make sure that this data is kept safely, processed securely, and stored in a way that makes it impervious to theft, hacking, and other kinds of misuse. She stressed the importance of maintaining the privacy of market users' data, noting that derivatives data is a singularly lucrative target for hackers worldwide. DLT has the potential to offer privacy solutions as it can be tailored to suit different information ecosystems and adapted so that only certain market participants have access to certain kinds of data. 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 the network on a continuous basis. She also noted that the distributed nature of information on the network means no longer relying as heavily on single repositories or a handful of data repositories whose loss can create enormous systemic fallout, economic cost, and potential loss of trust in the market.

Ms. Hoffman-Childress explained that blockchain encryption prevents sensitive information from getting into the wrong hands and being misused or even forgotten. She said that the real issue with hacking lies in the weakness of the systems that hold the data and not the blockchain itself. Ms. Hoffman-Childress stated that quantum computing is on the horizon, and companies like IBM are working on quantum encryption, which will use the principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked. She noted that DLT is also known for its ability to create an encrypted and immutable digital record of transactions. She explained that today the most widely used hashing algorithm is SHA-256, which can convert data into an encrypted "fingerprint" that represents that data's digital signature, and that SHA-256 represents a one-way hash that means it is impossible to reverse engineer and retrieve the underlying data in original form. This helps protect the data's integrity so if the underlying data is changed in any way, a new hash is generated. DLT can thus enable efficient storage and filing of documents.

Ms. Yadav then discussed how DLT can be useful in the custody function, which is essential to financial markets and derivatives. DLT networks that can securely verify user identities and trades and automate signals to custodians and warehouses that direct the transfer of assets represent a way to more fully automate the custody function and increase efficiency.

Ms. Hoffman-Childress said that DLT can be a game changer for audit and compliance, which needs an indelible record of all key transactions over the reporting period. DLT can lower the cost of audit and compliance. She stated that technology rapidly changes, therefore, regulators should not regulate the technology itself but rather its outcomes and impacts on individuals. She presented four questions for policymakers to consider regarding DLT:

1. Do DLT-based information verification standards meet various legal standards for data privacy and security in derivatives?
2. For interoperability, will markets demand just a handful of encryption standards?
3. How should innovation in encryption take place, where a handful of standards support financial markets?

4. Should the CFTC lead international standard-setting in relation to data privacy and DLT?

After the presentations, Chairman Gorelick asked the panelists what short-term developments should the CFTC focus on in the next year or two. Mr. Levy said that 2025 is the time where many individual value propositions will come together and create super-value based on this new technology space. Ms. Yadav identified the lack of standards internationally as a big issue. Ms. Hoffman-Childress recommended that the focus be on the outcomes that we want, and said the technology will fall in place. Mr. Levy said cross-border initiatives should not be the focus at this time, and that record safekeeping and custody are important issues. Mr. Stein asked about best practices in anticipating the power of quantum computing, which may make data less secure in the future. Ms. Hoffman-Childress stated that question keeps her up at night, but IBM recommends quantum encryption. The panelists also discussed the variation in international responses. Ms. Hoffman-Childress said some countries that have blocked crypto, allow blockchain for business.

[Lunch Break]

IV. Panel III: Automated and Modern Trading Markets Subcommittee Presentation

Following the lunch break, Chairman Gorelick introduced the third panel. Ms. Crighton gave a presentation on FIA's best practices for managing risks associated with electronic and automated trading systems. Ms. Crighton noted that FIA engaged for nearly a decade with futures exchanges, market participants, and international regulators on the development of best practices to mitigate the risks of electronic trading. These efforts have been in response to growth in exchange volumes and various market events. FIA believes 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. She outlined the principles of FIA's best practices, including pre- and post-trade risk controls.

Ms. Crighton then presented trends and themes identified in various FIA market surveys conducted between 2010 and 2018. Exchanges were surveyed on their provision of risk controls and market participants were surveyed on their use of FIA recommended controls. She noted that the surveys demonstrated, among other things, that there has been a substantial increase in implementation of market integrity controls since 2010, including price banding and exchange market halts, and that there has been generally positive feedback to industry initiatives and responsiveness to identify and self-solve industry risks. Ms. Crighton said that as markets and risks evolve, the industry response is also evolving. FIA has identified the following themes: (1) automated access to risk controls; (2) more granular pre-trade risk controls, specifically at the account and individual trader level; (3) potential new "buying power" (client creditworthiness) limits; and (4) improvements in exchange certification and testing.

Next, Mr. Kapani gave a presentation on how ICE thinks about risk across all of its futures exchanges and the foreseeable future. Mr. Kapani outlined ICE's risk controls philosophy, which is applicable across all its exchanges, covering all futures and options products. He noted that ICE's risk controls focus on preventative pre-trade measures and post-trade detection and mitigation, real-time management of risk, granular control at different levels

of aggregation, and tighter integration with third-party and in-house risk systems. Mr. Kapani then described ICE's controls in different categories, including market controls (e.g., price banding or collars that warn about or reject orders that are outside the band of current market value and circuit breakers), clearing member managed controls (e.g., that allow clearing members to control the kind of limits to give participants based on their risk and sophistication), and trading firm managed controls (e.g., self-match protection that prevents users from a given company or desk from trading with each other). He then discussed detection and mitigation tools that are in place or are being developed, including kill switches, FIX API, and breach alerts. He also explained how well ICE's risk controls performed during the Saudi bombing event.

Following the presentation, Mr. Levy asked whether there are evolving initiatives or issues on the horizon, in terms of future technology, that are predictive of future problems. Mr. Kapani said that ICE conducts predictive analysis based on historical data, which trigger alerts on the screens of its market supervision teams when there are exceptions outside the norm, whether at the market or participant level. For example, the statistical-based tools that ICE has built, combined with monitoring by its market surveillance and supervision teams, allowed ICE to handle the Saudi bombing event. Mr. Lothian asked Mr. Kapani to explain how ICE's circuit breaker tools functioned during a recent downward move of 16% in a day in Bitcoin futures, an illiquid market. Mr. Kapani said that there were no sudden jumps that triggered circuit breakers that day, and that price collars and limits were set appropriately for participants and worked as designed.

Ms. VedBrat expressed concern about unanticipated sharing of information and asked whether ICE shares information about an end user's portfolio beyond a particular customer's FCM relationship in the event of a breach. Mr. Kapani responded that portfolio information is not available in a general form, and is only available to the participant and their particular FCM. Mr. Kapani noted that it would be a major cyber incident if a firm had multiple FCMs and there was any sharing of the portfolio information across the FCMs. With regard to the Bitcoin futures market, Ms. VedBrat asked whether it has its own default fund. Mr. Kapani explained that Bitcoin has a $35 million separate waterfall before the regular risk waterfall kicks in, and additionally, ICE has separate insurance for breaches related to Bitcoin or virtual currencies. Ms. VedBrat noted that if there are clients who made a decision that they do not want any exposure to Bitcoin, they shouldn't have any indirect or unintentional exposure. Mr. Kapani stated that ICE received a lot of feedback when they launched the product, and structured the product accordingly.

Commissioner Quintenz stated that there is often the perception that if there is not a new regulation there is not any advancement in the addressing of risk by the marketplace or private sector. He noted that the presentations show exactly the opposite—that the industry has been all over these types of risk due to a strong business interest and ecosystem interest in addressing these risks at the exchange level, clearing member level, and firm level. Commissioner Quintenz complimented both presenters and the actions their firms have undertaken and is interested in any current or future analysis of the data gathered by FIA.

[Break]

V. Panel IV: Cybersecurity Subcommittee Presentations

Following the break, Chairman Gorelick introduced the fourth panel for presentations on the FSSCC's Cybersecurity Profile and the current approach to vender risk management, the challenges of that approach, and possible alternatives to consider. Mr. McHenry began his presentation by noting that the purpose of the presentation is to have the TAC consider at its next meeting the Cybersecurity Subcommittee's proposal that the CFTC join other oversight organizations in issuing a statement of support for the FSSCC Cybersecurity Profile. He stated that a comprehensive overview of the profile was presented at the TAC meeting on March 27, 2019. Mr. McHenry said that regulators in the financial services sector have recognized the risks posed by cyber threats and have responded with strong risk and principles-based regulation. However, firms are finding that a significant amount of their resources are needed to interpret and evaluate these regulations at the expense of the actual application of security controls. So members of the FSSCC sought to coordinate an industry-wide effort to create a more organized and consolidated catalogue view of regulatory standards, and to map this catalogue to the highly regarded National Institute of Standards and Technology's (NIST) cybersecurity framework.

Following this overview, Mr. Magri provided a graphical depiction of the reconciliation process, which maps approximately 2,300 regulatory provisions against the NIST cybersecurity framework. The FSSCC's architecture is based on NIST's cybersecurity framework and the 2016 guidance on cyber resilience for financial market infrastructures issued by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO). Diagnostic statements are used to synthesize and simplify overlapping requirements from the nine federal financial services regulatory agencies. A nine question impact questionnaire is used to scale the profile to both large and small firms, according to the firm's impact on the global, national, and local economies. The profile was a collaborative endeavor of 150 financial institutions with input from the nine federal regulatory agencies and the public.

Next, Mr. Harrell delivered a presentation on the current approach to vendor risk management, challenges with the current approach, and a potential new approach that the subcommittee should consider in light of these challenges. Mr. Harrell stated that the sophistication, frequency, and scale of cyber attacks against the financial services sector have made resiliency a priority for many jurisdictions. He explained that resiliency refers to the practices and disciplines that enable firms to provide products and services to the marketplace in the face of disruptive events, regardless of the nature or origin of such events by anticipating, preventing, recovering from, and responding to such events. Mr. Harrell said that several supervisors (e.g., the Bank of England, Financial Conduct Authority, Prudential Regulatory Authority, Monetary Authority of Singapore, and Australian Securities and Investments Commission) have released consultative documents with their position on resiliency, and additional standard setting bodies are identifying opportunities to support the sector in its resiliency efforts. He noted that it has been uniformly agreed that a service-based approach to resiliency must be taken in order to assure that the sector can continue to provide products and

services to the marketplace in times of extreme market stress, which means that not only the firms providing the product or service but the entire supply chain (i.e., vendors) used to deliver these services must have a certain amount of resiliency built into their operations.

Mr. Harrell then described four current vendor management challenges. One challenge is risk visibility and questionnaire fatigue; it is burdensome for vendors to complete lengthy questionnaires and the questions provide a limited understanding of the true business risks that a firm faces when using a vendor in terms of its resiliency in times of market stress. Second, vendors with multiple financial clients find it difficult to be compliant across multiple firms' policies and standards. Third, intellectual property protection, vendors are hesitant to disclose technical details or design vulnerabilities of their applications or services because this information may compromise the application or service if accidentally leaked to the public. Fourth, there is an uneven contractual leverage between small and large vendors and small and large financial firms. In light of these challenges, the subcommittee believes that there must be a different approach to vendor management to create an equitable risk balance between the financial institutions and the third party vendor. Mr. Harrell noted that a potential new approach would be requiring vendors that engage in business with the financial services sector to be certified or accredited against a recognized industry standard where the requirements and frequency of the certification is dependent on the size of the vendor and the level of risk that is inherent to the financial marketplace. He stated that the industry may realize several benefits from this approach, such as reduced questionnaire fatigue, harmonization of cybersecurity policies and standards across multiple firms, simplified contractual language relative to cybersecurity, and a greater level of resiliency assurance than the current vendor management model.

Chairman Gorelick asked about the goals of the FSSCC Cybersecurity Profile working group with regard to the CFTC and whether new rules and regulations or changes to auditing functions would be required. Mr. Magri replied that the working group is requesting that the CFTC issue a statement of support, and longer term, that agencies take a look at the profile and, if they are considering new regulations or guidance, put it out for public review and comment. Alternatively, they would appreciate a conversation or public comment period with reference to the profile, so that they have the opportunity to work with the agency to develop a mapping of regulations going forward. Mr. Magri also noted that examiner training is important because the working group wants the profile to work not only for firms that use it but for examiners as well. The participants discussed some of the challenges with the current vendor management model, whether industry participants can be satisfied with certification or accreditation standards, and whether more standardized disclosure by vendors themselves might provide an alternative solution.

VI. Closing Remarks

Chairman Gorelick thanked everyone for their participation. Commissioner Quintenz expressed his sincere thanks for everyone's hard work and robust participation.

Ms. Tente adjourned the meeting at 3:28 p.m.

I hereby certify that the foregoing minutes are accurate.

Richard B. Gorelick

Richard Gorelick
Chair, Technology Advisory Committee

1/9/2020
Date