

2023 NFA Member Town Hall
May 5, 2023

Joe McCarthy:

Good afternoon, everyone, and welcome to NFA's Town Hall Webinar. My name is Joe McCarthy and I'm a Senior Communications Specialist here at NFA's External Affairs and Communications Department. Before we kick off today's program, I have just a few housekeeping notes. With regard to format, we'll begin today's webinar with a brief update on recent initiatives at NFA. Then we'll spend the remainder of our time today answering questions from you, our Members, that you can submit.

To submit a question, locate the box labelled Ask a Question on the left side of your webinar screen, type your question into the box and click send. We're able to see the questions as they are submitted, so you could submit your questions at any time throughout the webinar. We will answer as many questions as time allows. Should we not get to your question though or if you asked a firm-specific question, an NFA staff member will reach out to you following the webinar.

Lastly, a recording and transcript of today's webinar will be available on NFA's website in the coming weeks. The Town Hall's purpose is to provide an opportunity for you to engage with NFA's leadership and members of our Board. We want to hear from you. I encourage you to submit a question - any question that you may have about what's going on here at NFA.

Member input is critical to NFA's ability to effectively regulate the industry. While events like this webinar are one-way NFA engages with Members, NFA also has several advisory committees that offer guidance on rulemaking and other initiatives. Our FCM swap participants, CPO, CTA, and IB Advisory Committees work to bring industry representatives together with NFA to establish effective, efficient, and balanced regulation. Education is also critical to NFA's mission. NFA recently hosted our Member regulatory workshops in New York and Chicago. We had well over 400 people attend those two in-person events. If you couldn't make it, the archive materials from those two sessions are available on NFA's website.

NFA will also hold webinars and provide educational materials on a variety of topics to ensure Members understand and can meet their regulatory obligations. I encourage everyone to check out NFA's website to see our latest offerings and to subscribe to our communications so you can stay in the loop on all upcoming educational opportunities. I'll now turn the floor over to NFA President and CEO Tom Sexton and later to some of my NFA colleagues to talk about a handful of important initiatives. Tom?

Tom Sexton:

Thank you, Joe, and welcome to our Members joining us today for our seventh Member town hall. As Joe mentioned, Member input is critical to NFA's ability to effectively regulate the derivatives industry. When faced with regulatory challenges and issues, we need you, our Members, to help us find practical regulatory solutions. We can all appreciate that today's global marketplace is rapidly changing and the pace of these changes appears to be increasing. To address them, close cooperation and coordination with other regulators, both domestic and international, is vital to fulfilling our mission of protecting investors and ensuring market integrity.

The need for effective and efficient regulation is greater than ever. Given NFA's important role in the US financial regulatory structure, it is essential that we work closely with our valued regulatory partner, the CFTC, to resolve regulatory challenges and issues. The CFTC also works diligently to ensure that NFA is fulfilling its regulatory responsibilities. In a moment, several of my colleagues will discuss recent initiatives and reminders important to you, our Members. I want to encourage you to ask questions during today's webinar. Our knowledgeable staff and leadership team will answer as many questions as possible during the time we have today.

Before we move on to the updates, we want to first recognize our colleague, Dan Driscoll, who in mid-March was inducted into the FIA Hall of Fame. This is a well-deserved honor for Dan, and we're proud to have him joining us today for this town hall. I will now welcome NFA's Board Vice Chair, Don Thompson, to provide a few remarks. Don, turn it over to you.

Don Thompson:

Okay, Thanks, Tom. I'm very proud of what the NFA staff, both collectively and individually, has achieved since we last held this Member Town Hall. Staff oversee and educate our Members build critical technology, advanced innovation, and recruit talented, diverse individuals who support the very important mission of the NFA. Additionally, I'm always impressed with how effectively and pragmatically NFA staff respond to regulatory challenges. This was especially obvious during the pandemic, with its many challenges which resulted in various relief from rulemakings to adapt to the changed circumstances during the pandemic.

Given NFA's important role in the US financial regulatory structure, it is essential that the CFTC closely reviews and monitors NFA's activities to ensure that NFA is fulfilling its regulatory responsibilities. I'm excited to see the continuation of this successful relationship with the CFTC. Back to you, Tom.

Tom Sexton:

Thank you, Don. Don has kindly made himself available to answer Members' questions later in today's program. Before we begin answering

questions, though, I'd like to ask a few of our officers and other leaders to discuss some recent NFA initiatives. I'm going to turn it over to Katie Clapper, who's a Managing Director in our futures compliance area. Katie?

Katie Clapper:

Thanks, Tom. Good afternoon, everyone. I wanted to touch on, today, NFA's third-party service provider guidance and initiatives. So risks associated with third-party service providers including the cybersecurity risks they pose, has been an area of focus for some time, and of course, our top of mind in the wake of recent ION events. The cyberattack on ION earlier this year underscores the need for strong cybersecurity practices and a robust supervisory framework surrounding the use of third-party service providers for regulatory functions.

In 2021, NFA issued Interpretive Notice 9079, which outlines minimum supervision requirements for Members who use third-party service providers for regulatory functions that the Member would otherwise undertake themselves. The interpretive notice requires that Members have written supervisory policies addressing several key areas, including an initial risk assessment, onboarding, due diligence, ongoing monitoring, termination, and record keeping. So, I'll touch on a few of these areas with a focus on what Members need to be thinking about from a cybersecurity perspective.

First, an initial risk assessment. Members need to consider the risks of outsourcing a particular regulatory function, including information security considerations, and determine that they're comfortable that these risks can be sufficiently mitigated. For example, a Member should think about the type of information that the third-party service provider will need access to and whether it's confidential information or customer PII.

Next, Members should undertake onboarding due diligence to consider if a particular third-party service provider has the expertise to carry out a regulatory function and the level of due diligence to be relative to the risks associated with outsourcing. So that heightened scrutiny is applied if the third-party service provider is critical to carrying out a regulatory obligation or holds critical or confidential data. Examples of consideration would include the background of the particular vendor, its information security practices and business continuity, disaster recovery, and contingency planning. Ultimately, Members are responsible for fulfilling their regulatory responsibilities, even if a function is outsourced. So thorough due diligence is vital.

After onboarding, there's an expectation of continued ongoing monitoring. Using a risk-based approach, Members should review to ensure that third-party service providers are appropriately carrying out the function. And the

scope and the frequency of this review may depend on the function. So a third-party service provider undertaking critical regulatory sensitive data may require more frequent or detailed review. And again, Members need to consider IT security, business continuity, disaster recovery, and contingency plans. And also evaluate the reliance on a particular third-party service provider and consider alternatives or a contingency plan if the third-party service provider has a failure due to a cyber-attack or not.

Finally, in the event that the relationship with the third-party service provider is terminated, Members must require that the third-party service provider gives adequate termination notice so the member can find a backup and make steps to ensure the third-party service provider doesn't have access to confidential data after the termination.

In conclusion, Members should continue to focus on the supervision of third-party service providers and ensure that cyber risks are considered in their assessment. NFA will also continue to review its interpretive notice regarding the use of third-party service providers for regulatory functions to determine if any updates are needed based on recent industry events. Next, I'll turn it over to Dale Spoljaric, who will discuss cybersecurity initiatives.

Dale Spoljaric:

Thank you, Katie. So, this afternoon, I'll take just a few minutes to highlight the key elements of an effective cybersecurity program that are outlined in our interpretive notice 9070, which became effective in early 2016. So, anyone who has read both the third-party service provider and cybersecurity interpretive notices, side by side, will notice a similar approach in the requirements and a direct connection between the two. In terms of approach, consistent with the third-party interpretive notice that Katie just described, the cybersecurity interpretive notice also applies to all Membership categories and outlines a flexible framework for how best to diligently supervise cybersecurity risks. And the foundation of an acceptable framework is a written program that covers key topical areas and processes that should be in place at the Member.

So, what are those key areas? Well, everything starts with an initial risk assessment to identify threats and vulnerabilities to the firm's systems and data. This effort, admittedly, will require a wide reach, knowing all of the physical hardware and use by the firm, the software running on all the machines, the connection points to the firm's systems, and where all the critical data is maintained, is a significant undertaking. Fortunately, there are a number of professional associations in this area that provide specific best practices and standards to follow.

Along with our interpretive notice, we've also published a Frequently Asked Questions document available on our website that identifies some of those

resources. So, things like the NIST Cybersecurity Framework, for example. Once threats and vulnerabilities are identified, the firm will need to put in place protective measures to safeguard the firm's systems and data. This area in particular is one where there is no one size fits all solution. The protective measures chosen by the firm will be highly dependent on the firm's operations, technology, and interconnectedness with the outside world.

Next, the firm's program must also include an incident response plan. Almost all cybersecurity experts will say it's not a matter of if you will experience a cyber incident but rather when it will happen. So, it is critically important for everyone to know their role and the steps to take to address any event. One such step will be to determine if notification is required to customers, law enforcement, and even regulators. Our interpretative notice does include a narrowly tailored provision that requires the Member to notify NFA of certain incidents that result in a loss of customer or counterparty funds, the loss of the Member's own capital, or in the Member providing notice to customers or counterparties under state or federal law.

Responding to an incident and safeguarding against an event in the first place is dependent upon training employees. Our interpretive notice also requires that training be provided upon hiring and at least annually thereafter. The firm's written program should also describe the ongoing education and training efforts for cyber security as well. In order for the firm's program to remain effective, the interpretive notice requires that the firm review its program at least once every 12 months, which may be done internally or by engaging with an external consultant or specialist.

Which brings me to my final point, and that is the connection to the third-party service provider that Katie mentioned. Whether the Member chooses to use an external party to perform a review of its program or a vendor to provide support for other non-cyber-related operations, the Member should perform due diligence on any third party that connects to the firm or has access to firm data. That concludes my piece of the presentation, and I'm happy to pass it over to Katie Owens to talk to you about multi-factor authentication.

Katie Owens:

Thanks, Dale. So earlier this week, NFA began its rollout of multi-factor authentication or MFA. For those of you that have logged on to some of our external systems, you might notice that the sign-on screen is very different than what it previously looked like. MFA - so what is MFA? So, MFA is a login method requiring our users to provide an additional verification factor to gain access to a system beyond a username and password. You may already be familiar with this for your other systems that you log into such as your bank account or other secure websites. For NFA system users, the

additional factor will be a time-based one-time passcode, or TOTP for short, which is delivered to you via email, text message, or authenticator app. We're providing some options for that.

Our users will be able to select the preferred option when they enroll in MFA, and you'll only need to do this once. So why is NFA rolling out MFA? Well, to keep your account more secure, MFA is one of the most effective security controls we currently have available. Passwords are increasingly and easily stolen, guessed, or hacked. MFA ensures that accounts remain secure even in the event of a password being compromised. Christie, I'm going to pass it on to you to talk some more about MFA and what NFA is doing.

Christie von Ohlen:

Perfect. Thanks, Katie. So first, I'll share a little bit about the launch. So as Katie alluded to, thanks to the rollout of MFA, as of this Monday, all NFA systems, with the exception of Windjammer, now have a new look and feel. Rollout of MFA itself also began on Monday, May 1st for our FCM and our [inaudible] users. So the next time those users log into an NFA system, they'll then be prompted to enroll in an MFA. Rollout will then expand to swap dealer users on May 7th, IB users on May 14th, and then all other users on June 4th. For more information on MFA at NFA, please visit the NFA home page. There you should see a banner across the top of the screen that links to a page containing a list of FAQs that we hope you find helpful.

And then additionally, if you have other questions on MFA, we're happy to help. Please reach out to NFA's Information Center and we can get you the info you need. And now I'll turn it over to Mike Schorsch from our legal department, who's going to talk a little bit about NFA's Compliance Rule 2-51. Mike?

Mike Schorsch:

Thanks, Christie. So, NFA's Board of Directors recently adopted a new rule, Compliance Rule 2-51, which is entitled Requirements for Members and Associates Engaged in Activities Involving Digital Asset Commodities. It goes into effect on May 31st. This new rule was adopted because a number of NFA Members engage in business activities that involve digital assets, including spot transactions. But NFA's rules, for the most part, are limited to a Member's commodity interest business, the futures swaps, and retail forex. In other words, NFA's rules do not cover spot market activities in digital assets. And this puts NFA in an untenable position if we had a Member firm which was involved in digital asset commodity spot activities and engaged in fraud or similar misconduct. Because we would not have a clear rule to take action against that Member for that misconduct.

Compliance Rule 2-51 is meant to close that gap. It has four key elements. First, it prohibits fraud. Second, it requires a Member to act in a manner consistent with just and equitable principles of trade. Third, it requires compliance with interpretive notice 9073, which in turn requires most Member firms offering digital asset transactions to provide certain disclosures. And fourth, and finally, Rule 2-51 requires diligence supervision over digital asset commodity activities.

The rule applies to all Members but only covers activities and digital asset commodities rather than all digital assets. The rule specifies that this means bitcoin and ether. These are the two digital assets that are most accepted as commodities, and they are the only digital assets which are the underlying for listed derivatives on CFTC-registered contract markets. Between the two of them, they also make up the majority of digital assets by market cap.

The CFTC already has anti-fraud jurisdiction over digital assets that are commodities. And the commission has brought a number of enforcement actions related to spot market activities in Bitcoin and ether. So, the new compliance rule brings NFA's authority closer into alignment with the CFTC in these important new markets. But it also allows NFA to go further by requiring a Member to act in a manner consistent with just and equitable principles of trade and requiring a Member to supervise these activities, which is an important component of ensuring that misconduct does not occur. This rule is designed to give NFA more tools to protect the public and to require Members that are engaged in spot digital asset commodity activities to adhere to the same high standards required for their commodity interest business. And now I will pass it over to Val O'Malley, who will talk about on-site exams.

Val O'Malley:

Thanks, Mike. I just wanted to give a brief update on our exam process. At this point, we are back on site for the vast majority of our examinations. For a lot of our exams, we're taking what we call a hybrid approach. As we've done in the past, what we'll typically do is exam teams will announce an exam, send out a pre-exam questionnaire, and have discussions with firm personnel. This allows teams to get an understanding of the firm's operations and to set the scope for our testing. From that, teams will compile their requests and send out a document request list. Using this hybrid approach, rather than go out to a firm right away, what we'll do is obtain documents from the firm and then do a substantial amount of work at NFA's offices prior to going to the firm's location.

It's really important during this time that the firm be responsive to questions and provide documents timely so teams can begin their reviews. The amount of time spent on site by teams will depend on the size of the firm

and the scope of the exam. For some firms, this may mean that a team may be in the field for a couple of days to a week. And for larger firms like FCM, FTMs, and swap dealers, it may be more like two to three weeks. With using this hybrid approach, we're really trying to make the most of the time that we are at firms and complete testing that is better to be done in person. So, this may include things like testing of internal controls and conducting various walkthroughs with firm personnel. So it's important that the right firm personnel are available and in the offices when we are on site.

Being at the firm allows us to give on-site training to our newer staff. As like many organizations during COVID, we did experience some turnover and we really feel that it's important for these staff to be in the field. Being on-site also allows teams to collaborate on what they're seeing in their reviews and discuss whether additional areas of testing need to be performed. Teams can make additional requests from the firm while on site. As we've done in the past after being at the firm, teams will then finish the remainder of the exam back at NFA's offices. During this time, teams may make additional requests for records and have follow-up discussions with the firm prior to issuing the exam report.

So, all that being said, the very beginning of the exam process and the end of the exam process is relatively the same. You may just see a difference in when exam teams begin asking questions relating to their testing and when coming on site. And we hope that this makes the exam process more efficient for both us as well as our Members. And now I'll turn it back over to Tom.

Tom Sexton:

Thanks, Val, and thank you to those who discussed these important topics today. We look forward to continued collaboration with our Members on these topics, and we will keep you apprised of developments as they may occur. Now let's get into your questions. Joe, I'm going to ask you to please moderate this portion of the program, our Q&A. Joe?

Joe McCarthy:

Thank you, Tom. Tom mentioned this is the main portion of our webinar. We've seen a few questions trickle in here. I encourage you to ask any questions, leveraging the resources we have from NFA on the call. To submit a question, locate the box labelled Ask a Question on the left side of your webinar screen, type your question in the box, and hit send. We're looking forward to seeing those questions come through. Again, if you have a question following today's webinar, you can find the contact information to NFA's Information Center online on NFA's website and I encourage you to reach out there. So, we'll start with our first question. Carol, I'll ask you to join the call here. Asking a question regarding enforcement actions, any trends that we saw in the enforcement area last year?

Carol Wooding:

Thanks, Joe. I mean, the first thing I'll say is that the activity of our business conduct committee was relatively consistent with what it's been in the last few years. In last year, in 2022, they actually issued 18 disciplinary complaints. I think it's notable that 11 of those complaints involved IBs. And even more notable, I think, is that nine of them alleged violations that included a failure to maintain required communications. And those were by [inaudible] and staff views. These communication records is very important and very useful tool for the Member to use itself as part of supervising their APs activities. So, we will be continuing to look at those areas in our upcoming exams over the next year.

Joe McCarthy:

Thank you, Carol. Tim, I'll turn to you. And MFA is a timely topic for us, but wanted to talk a little bit about that. A question regarding the new sign-in process using multi-factor authentication. Can you talk a little bit about the role of the security manager or will this role still remain?

Tim McHenry:

Yeah. Thanks, Joe. Great to hear from all the security managers out there. That role will indeed still remain and the security managers will have all the same functionality that they're used to. So that includes adding accounts, deleting accounts, and updating accounts. So that function, that role is still critical and that still will remain in place even with the new sign-on process.

Joe McCarthy:

Thank you, Tim. Yvette, I have a question here regarding the futures industry proficiency exam. So FINRA administers that exam, the Series III, and it currently allows for online testing. Do you know if this option will be a permanent option or do you have any other insights you could provide there?

Yvette Christman:

Yes, Joe can. So online testing is not going away. However, beginning this summer, and the date is still to be determined, candidates will need an approved accommodation to take any of the NFA exams online. The accommodations will be available for candidates who have underlying medical conditions or who reside more than 150 miles from a testing center. Once the final date is set, NFA will send out a notice and FINRA will also post information on their website with detailed information about the change.

Joe McCarthy:

Thank you, Yvette. Dale, a question here regarding swap dealers who are also registered with the SEC as security-based swap dealers. Can you talk

a little bit about the NFA coordination with the SEC staff on these examinations?

Dale Spoljaric:

Sure thing. Thanks, Joe. So, 2021 was a big year for existing swap dealers with the capital regulations going live as well as security-based registration and regulatory requirements associated with that. Since that time, I can promise you that we have had many conversations with SEC staff. We recognize that many of our swap dealers, the CFTC-registered swap dealers, are also security-based swap dealers and there is some regulatory overlap. So, our primary intent of coordination with SEC staff is to make sure that we're aligned and we're trying - and trying to reduce some of that regulatory overlap, sharing our thoughts, sharing our observations, and making it as seamless as we can, as seamless as an examination can be when we come in and do on-site work. So I'll just say that, yes, please know that we do coordinate with SEC staff.

Joe McCarthy:

Awesome. Thank you, Dale. Katie Clapper, I have a question for you. This is in regard to the annual questionnaire. Wondering if there's going to be any updates to expect into the annual questionnaire. I don't know if you could provide any insight into that area.

Katie Clapper:

Sure. So, the annual questionnaire is a very valuable tool for us that we use to assess our Members and determine if there's good exam candidates. So, it's something that we certainly look to frequently for any updates in trends. And we have recently started to look at some updates related to digital asset activity and ask a few more questions in that area. So, stay tuned for when those will roll out. But we'll certainly give notice when that occurs.

Joe McCarthy:

Awesome. Thank you, Katie. Karen, I was hoping I could ask you a question here. This is in regard to NFA's Member education initiatives. Can you just talk a little bit about, one, the scope of our Member education and how NFA develops those for the future?

Karen Wuertz:

Sure, Joe. One of the things I wanted to start with to just when we talk about Member education is, one of the pillars of our mission and something that is ingrained in part of our DNA and part of our philosophy is that we want to make sure that our Members understand their regulatory obligations. We've never taken a position where we want to be what I would describe as a got-you regulator. We think it's much more effective and better for the industry if we spend a lot of resources providing education about our Members'

regulatory obligations, again, rather than catching someone violating our rules.

So, with that in mind, and again, that's just such a critical part of our DNA and we're always looking for opportunities to educate our Members. And today is a perfect example of that. Joe, you mentioned early on our Member workshops where we had over hundreds of participants. And the resources from that Member Workshop are available on our website. Quite honestly, one of the biggest educational resources we have is our website. There's a tremendous amount of information regarding all of our regulatory obligations. So, if anyone has any questions, that's where I would advise our Members to go to first for any information.

We talked about our Info Center, that's another resource. In addition to the Member Workshops, we're also looking for topical programs, and the way we get ideas regarding topical programs is from our Members. Other areas we look at when looking for educational programs is if we're updating the annual questionnaire or if we're updating a system, just like Katie and Christie talked about earlier, we did a specific educational short webinar to help our Members transition to the new MFA security system for our systems. So again, just a whole host of programs that are available.

One other initiative that we've been doing for several years is after each of our Board meetings, we provide a publish a Board Update Video. So that gives Members more of a high level of the various initiatives that the Board is considering on its agenda. So, Joe, I think I'll close there. But again, one other - maybe I'll say one other thing, if Members have any ideas for topics that we should cover, we welcome those ideas and we'll put those programs together. So, I'll close there, Joe.

Joe McCarthy:

Thank you, Karen. I just want to remind everyone too, as Karen mentioned, our website is a good resource. This webinar and a transcript will be available as an archive version on the website in the coming weeks. So, I encourage you to access that net - that link, that information is available to everyone, even if they haven't registered for the webinar. So, I encourage you to share that with your colleagues who are unable to join us today. I have a question here regarding just NFA exams and when Members should maybe expect exams, again, the frequency of exams. Katie, I don't know if you want to give a little bit of perspective from the futures side.

Katie Clapper:

Sure. Thanks, Joe. So, the frequency of exams, I would start with, depends on the risks presented. We take a risk-based approach for our exams, and so that really largely drives when an exam of a particular Member may be scheduled. It is relevant to raise that FCMs are required to be examined on

a nine-to-15-month cycle. So, we are going to probably see our FCM firms around annually, whereas other registration categories, we're looking at various risks to determine when to schedule an exam.

Joe McCarthy:

Thank you, Katie. Looking over, just trying to get a sense of the questions here. I have another question. Tim, this is kind of related, again, to MFA. I know this is something that we've maybe been hearing a little bit about. Again, back to that security managers' crowd, are they able to reset their user accounts? Could you provide just a little bit of insight there?

Tim McHenry:

Yeah. Thanks, Joe. Yes, indeed, the security manager will still be able to change passwords, reset locked accounts, and they can even change the method of authentication for the dual factor. So, they'll continue to play that critical role. They'll be the go-to person for that kind of maintenance in terms of accessing NFA systems for your firms. So that will indeed continue to be their role.

Joe McCarthy:

Thank you, Tim. Carol, I want to turn it over to you. This is a question in regard to 2-51 Mike gave an update a little bit earlier. Just talk a little bit more about the monitoring efforts of NFA and its relationship to the Forex digital assets.

Carol Wooding:

Yeah. So, 2-51 is actually directed at spot digital assets. So, if they involve Bitcoin and Ether and our Members are involved in it, that's what 251 covers. It's not intended to cover the derivatives futures products that are trading on the regulated exchange. In terms of how we'll monitor our Member activities there, it'll be in the same way that we monitor Member activities for any of their activities that we currently have jurisdiction over. We'll review what types of interactions they have with clients and customers. We'll review the promotion material they send out. And I'm sure we'll be developing some additional testing that we can do that will be directed exactly at the spot digital asset market. The rule becomes effective at the end of May so our staff is working very hard on making sure that we're ready to go and start our oversight of that area.

Joe McCarthy:

Thank you, Carol. Yvette, I have a question, again, this is involving a question related to exams. So, this is actually the swaps proficiency requirement. We talked a little bit about Series III being able to be provided online, can you talk about the Swaps Proficiency Requirement if that's an in-person or online offering?

Yvette Christman:

Yes, Joe, I can. So unlike the Series III or any of the other futures exams, the swaps proficiency requirements has always been online and will continue to be online. So as we - as it stands now, there's no in-person training for that particular requirement.

Joe McCarthy:

Awesome. Thank you, Yvette. Dale or Mike, a question for you. The question Katie kind of tackled on the future side, just generally speaking about the frequency of exams. Dale or Mike, feel free to jump in. Can you just talk a little bit about, from the swaps' perspective, about what the frequency of exams would look like?

Mike Schorsch:

Sure. Thanks, Joe. This is Mike. So, for swap dealers, we also take a risk-based approach to scoping exams, which means the subject areas that will test and also on the timing of exams for swap dealers. We look at the risks posed by the swap dealers. Any previous deficiencies noted in exams. The types of markets that the swap dealers are in. The complexity of their business models. The types of clients they face. A whole host of information is factored into our decision on when to do an exam and what areas to test. So, there's no set model for how frequently an exam will happen. That said, firms that are subject to NFA and CFTC Capital requirements will see us more frequently than they have in the past, and we'll be testing compliance with capital and financial reporting for those swap dealers on every exam.

Joe McCarthy:

Awesome. Thank you, Mike. Don, I want to turn to you. I know we're kind of getting close here on time, but there's a question just regarding the latest from the Board. I was just wondering if you could, I know we have a Board meeting coming up, but I was wondering if you could share some of the topics that were covered during our last Board meeting.

Don Thompson:

Sure. I'd be happy to do that. At our February meeting, the Board was honored to welcome CFTC Commissioner Kristen Johnson. The commissioner addressed the Board regarding, among other things, cybersecurity, third-party service providers, the latest CFTC-MRAC meeting, and digital assets. She also stayed and took a bunch of questions from the Board, which we were very gratified that she made the time for.

On some administrative matters, we reelected Philip Capital's Maureen Downs to serve a one-year term as Chair of the Board of Directors. I was also gratified to be re-elected to a one-year term as Vice-chair of the Board. The Board also elected Public Directors and Member directors who will serve on next year's Executive Committee.

On other matters, the Board approved the adoption of NFA Compliance Rule 2-51, which we heard about earlier today. If you want to learn more about the Board meeting, you can watch the latest Board Update Video on NFA's website. We are currently preparing for our next Board meeting in later in May.

Joe McCarthy:

Awesome. Thank you, Don. Just, again, just to reiterate, the Board Update Video is available on NFA's website. Another one of those resources that I encourage you to subscribe to is NFA's Communications, if you've not done so already, so you could stay in the loop of those updates and other educational opportunities. I've gotten through the vast majority of the questions and kind of hit on some reoccurring topics. If we haven't gotten to your question though, I mentioned it earlier, an NFA staff Member will reach out to you via email. Again, the opportunity to reach out to staff is still available through the NFA's Information Center which you can find the contact information online. So, I appreciate all the questions. And with that, Tom, I'll turn the reins back over to you.

Tom Sexton:

Thanks, Joe. And as Joe said, we're going to close today's town hall. And I'd like to thank each of you for your participation. We hope that you found the information provided to be - today to be helpful. And the questions you asked are especially helpful to us and will assist us in better tailoring our Member educational programming going forward. As a reminder, you will be able to find a recording and transcript of today's town hall webinar on NFA's website in the coming weeks. In addition, as Joe indicated, if we didn't get to your question. We will respond to you by email. Again, if you ever have a question, feel free to reach out to any of us and we'll get you an answer as quickly as we can. Thank you again for participating today and have a good afternoon. Take care.