**MORGAN LEWIS PRESENTS 2019**

## Spotlight on SEC Cyber Trends – A Conversation with Carolyn Welshhans

## September 24, 2019

Tim Burke: Welcome everybody. Good afternoon. My name is Tim Burke, and I head the Securities Enforcement Litigation Practice here at Morgan Lewis. Welcome to our New York office, for those folks who've joined us live. We're delighted today to have with us Carolyn Welshhans, the acting head of, or Chief, of the Cyber Unit, at the SEC's Enforcement Division. We're going to have a very interesting program today for you, with respect to the ever-changing landscape of cyber regulation. We're also delighted to welcome our partner Ivan Harris, from our Washington office, who's going to be leading our discussion.

Tim Burke: And before we get to the program itself though, I did want to mention two things. First of all, by way of a preview, I wanted to let folks know that on November 14th, we're going to be conducting the Al Sommer lecture series at Fordham Law School. This year, it'll be a fireside chat with Commissioner Hester Peirce. I think it'll be a very interesting discussion. My partner Ben Indek will be moderating that one. So hopefully you can save the date, and join us for that event. November 14th, Lincoln Center. And then secondly, for the benefit of the folks here live in New York, this program is now the 11th annual program that Morgan Lewis has sponsored for the SEC Historical Society, and like the prior 10 programs, this will be preserved on the virtual museum of the Historical Society. So all of today's remarks will be there for you and others to visit. We're simulcast, or simul-broadcasting this through a webcast around the world today, and for that reason, we'd ask that folks locally save any questions that you might have until we're done with the recorded version of the program, so that we can have a pristine recorded version preserved for the archives.

Tim Burke: For those of you who are not familiar with the SEC Historical Society, I would encourage you to visit its virtual website, at sechistorical.org. It is the definitive repository of financial regulation history. It has both original pieces, and manuscripts, as well as oral histories, as well as presentations like the one you're about to hear today. So, if you haven't visited it, you really should, because it is an extraordinary resource for those who practice in this area.

Tim Burke: With that, I'd like to introduce Jane Cobb, the Executive Director of the Historical Society to kick us off. Jane.

Jane Cobb: Thank you Tim, and thank you for being on our board of trustees. We really appreciate Morgan Lewis's support over these 11 years, and hopefully for a partnership that will last into the future. Thank you too for coming in person here today. It's a beautiful day here in New York, although it is UN week, so it's a

little challenging to get around. But if you can't get here in person, we're happy to have you join us on the live webcast that's occurring right now. I have the pleasure of introducing the moderator, Ivan Harris, and Carolyn Welshhans, our special guest. And I'll have to use my cheat sheet here. Ivan's been with Morgan Lewis for I believe 12 years, now, and previously served at the SEC from 1998 to 2005. The last four of those years, he was the Assistant Regional Director for the Enforcement Division in the SEC's Miami office. Is that right Ivan?

Ivan Harris: You got it-

Jane Cobb: Hopefully.

Ivan Harris: Yeah.

Jane Cobb: And Carolyn, welcome. Carolyn is currently the Associate Director in SEC's Enforcement Division, and the acting Head of the Cyber Unit, as Tim mentioned. Prior to joining the Commission, Carolyn worked in private practice, and she graduated from Boston College Law School, and went to William & Mary College in Virginia. Welcome, and with no further ado, I'll turn it over to Ivan and Carolyn. Thank you.

Ivan Harris: Great. Thanks Jane. Thanks Tim. And thanks Carolyn for joining us today. I know it's a slow week at the Commission, and you don't have anything much going on, on this last week of the fiscal year, so we do appreciate it. So let's get into a discussion about the Cyber Unit. That's what we're here for today. For everybody's benefit, if you could give us a little bit of a background; what the Cyber Unit is, what its role and mission is, and, you could start with how it's staffed, that'd be helpful.

Carolyn W: Sure. And first, I have to give the warning that I'm sure everybody familiar with the SEC has heard, and that's that the opinions I express today are my views; they're not necessarily the views of the commissioners, the Commission, or its staff. So with that out of the way, the Cyber Unit was formed two years ago, in September. It actually was formed two years ago tomorrow, so this is a very timely event. The mission of the Cyber Unit is to enhance the SEC's ability to detect, identify, and investigate cyber threats, and cyber misconduct, by developing expertise, at the staff level in the Division of Enforcement, in a specialized unit. I mean I can talk about those in a few minutes. The staffing itself, there are approximately 30 attorneys in the Cyber Unit, including supervisors. They're in six offices, around the country, of the SEC. They are led by a Chief, a Unit Chief. Up until recently that was Robert Cohen, who was the founding Chief of the Cyber Unit. He recently left the SEC. And the Chief reports directly to the Co-Directors of the Division of Enforcement.

Ivan Harris: Okay. So it's one of the specialized units now, within the Division. Okay. And so, what other divisions perhaps does it work with on a regular basis. There're a lot of new issues that come up with cyber cases. There're a lot of interesting novel

issues that are coming up that involve markets, that involve broker-dealer activity, that involve... what's a security, what's not? Perhaps more so than some other specialized units. So can you give us an idea of how it's interacting with other divisions within the Commission, and other offices?

Carolyn W: Sure. So, there are a number of divisions and offices that we interact with, and it depends on the issue that's come up. Probably wouldn't surprise people to find out that when we're talking about initial coin offerings, for example, and whether something's a security, we have a lot of interactions with the Division of Corporation Finance. But we also interact quite a bit with Trading and Markets. We've had cases that've dealt with whether something is acting as an unregistered broker-dealer. In other contexts, lots of interactions with the Division of Investment Management, Office of International Affairs, General Council... There's quite a lot of collaboration across the divisions and offices. Also want to make clear there's a lot of collaboration across the Division itself.

Carolyn W: As I'd mentioned, as you'd mentioned, the Cyber Unit is a specialized unit, in enforcement, and for those of you who aren't aware, there are now six specialized units in the Division, approximately 20% of the Division's staff works in a specialized unit. The first five of these were formed in 2010, to develop specialized expertise in priority areas, for the Commission. And the Cyber Unit is the first one since then to be formed. But, there're certainly cyber cases being worked on throughout the Division, both within the unit, and outside of the unit, by those other 80% of the staff in the Division who are in what we call core enforcement. Some of those cases are cross-staffed with the Cyber Unit, on some there's consultation, and on plenty it's... you'll find staff in the regional offices and the home office, who are working on either cases that fall under the purview of the Cyber Unit, or touch on it in some way, because as everybody is aware in this day and age, it's hard to walk down the hall without running into something that has to do with cyber.

Ivan Harris: And similar to I guess the Enforcement Division, within those other divisions do you find staff members who are also specializing in these issues that affect kind of the cyber-type cases?

Carolyn W: Yeah, that's a great question. We are finding that expertise developing across the Commission. The Division of Corporate Finance for example has Valerie Sepanik, who was named in the last couple of years, maybe within the last year, as an associate, and a senior advisor on cyber issues, digital assets. But within all of the divisions, as these issues come up, and they're always different, but some variation on each other. For example, there are people in the General Counsel's office who tend to kind of stay up on these issues, and see them again and again, and that's who we deal with. Similarly across all of the other divisions, Corp Fin, Investment Management, there are people who have given a lot of thought to this space, and that we deal with a lot.

Ivan Harris: Interesting. So, outside of the Commission, these cases in particular, we'll talk some more later today about the cyber-security cases; the hacking and the breach-type cases, presumably involve a number of different law enforcement agencies. Are there other agencies that you regularly work with that you have perhaps regular working groups with that you can talk about? Not just the SEC, but other federal agencies that you're working with regularly?

Carolyn W: Yeah. And again, sort of like I mentioned, at the Commission, everybody is dealing with cyber issues, so we deal with state regulators, and state attorneys general, who have been very active in dealing with cyber issues, particularly initial coin offerings, that touch on investors in their states. We've also dealt with traditional law-enforcement partners, as you mentioned in kind of the hacking context, that it wouldn't surprise anyone. We're dealing with questions of fraud, or something of that nature, we deal with Department of Justice, FBI, Secret Service, postal inspectors, DOJ's Computer Crimes Intellectual Property unit. So there's a lot there. And in addition, the self-regulatory organizations also have cyber issues, where we're working with them in parallel.

Ivan Harris: Are you able to talk a little bit of kind of about that flow? For example with Secret Service, or postal inspectors, or FBI. Is it you're bringing cases to their attention? They're bringing cases to yours, equally? Or is it more that you're getting them involved when you think that the issues are broadening beyond the SEC's mandate, so to speak?

Carolyn W: I'd say it's a mix, which is true in a lot of contexts. There's a lot of stuff that we develop. We are the primary regulator in the security space, and so that's where our attention is really focused. It's where the SEC puts in a lot of effort to not just work the cases, but find the cases; figure out where we should be looking next. And so we bring a lot to the criminal authorities, but certainly they find things on their own, they hear things through people that they're working with in other contexts, and then bring it to us as well.

Ivan Harris: So, now that we've kind of established who it is, and what it does, give us I guess a sense of what the current priorities are for the Cyber Unit; the types of cases you're prioritizing now, and I'm sure that will launch us into some discussions for the rest of the hour.

Carolyn W: So I would divide it into kind of three main buckets. The first is initial coin offerings and digital assets, digital currencies. The second one is cyber security, and in that I would put the question of issuer disclosures, issuer controls for public companies, as well as controls for regulated entities; broker-dealers, exchanges, things of that nature. And then the final bucket would be trading, so people hacking to get material non-public information, or people breaking into, intruding into brokerage accounts, on an unauthorized basis, to conduct market manipulations. Or market manipulations conducted in other contexts, such as through electronic trading platforms. So I think those are kind of the three main

areas that we see, and that's how I tend to think about where we're seeing the misconduct, and where I think the attention is focused.

Ivan Harris: And is it kind of equally divided between the three, or do you find that the staff in the Cyber Unit is spending the majority of its time in one area, and the others are kind of less than that? Or how would you divide it up?

Carolyn W: I think they're all important. I think that you can see from the number of cases we brought and what's in the news, you tend to see more attention at least publicly focused on the ICOs, and the digital currencies. That's the thing that I think is kind of new. But that doesn't mean the other two areas are any less important. I think we've brought incredibly important cases in those spaces. They might take more resources, they might take more time, you may not see as many of them, but I think all three are important, and all three are areas that we're focused on.

Ivan Harris: So let's talk about them. And we'll start where you started, which is in the ICO digital currency-type space. And it's certainly the area that, you're right, has probably received the most attention, and had seen some of the most high-profile enforcement actions. Tell us a little bit about how the Cyber Unit approaches these cases, first from the question of whether it's a security or not, which I think has obviously received the most attention within that area. Is the current approach that basically all token offerings are presumed to be securities, unless you can demonstrate otherwise to us? How do you go about looking at those cases and analyzing them?

Carolyn W: So the short answer I'd give to your question is no, I don't think they are all presumptively securities. It's a common threshold question for us, and one that we take very seriously. It does depend on the facts and circumstances, and the thing we apply is the Howey Test, the Supreme Court case from 1946, asking the question of is an investment in an orange grove an investment contract? And that is still the law that we apply today, looking at the question of whether someone has invested money, which can include digital currencies, in a common enterprise, with an expectation of profit, generated by the efforts of a promoter, or some other third party. And that's I think the threshold question of is something a security, and then you get to the rest of, did it need to be registered? Did it meet an exemption? And then other potential violations that could flow from there.

Ivan Harris: An analysis that we've copied and pasted many times with the action memos, the Howey Test. So, you bring up the Howey Test though, and I guess what do you say to perhaps people who talk about the fact that laws written in the 1930s, cases issued in the 1940s, are really not equipped to tackle issues that involve the tokens issued and virtual currencies, and digital assets, and things like that? How do you respond to that?

Carolyn W: I think that's mistaken. I think, and I'm just going to geek out for a moment, since I'm at the Historical Society, and I think it's the perfect place to do it, I think our laws from the 1930s have held up very well. The question of whether something is a fraud, or whether something is a security, or whether someone needs to be registered; that's handled innovations in products for decades, and so the fact that what that product is now is a digital technology, I don't think is any different. And the fact that the 1933, 1934 Acts have been able to respond that way for so long I think is really beautiful and really great. It says a lot about the strength of those laws. Now that doesn't mean that we don't have to keep pace with the technology, but for example when the question is whether something is a security, what matters is the substance of the transaction or the offering, not the name; not whether it's a SAFT, or an ICO, or... a utility token. What matters, and what has remained the same, the reason for the need for registration, and that is to protect investors; to ensure that they get the information that they need to make informed investment decisions, and that if appropriate, those entities and individuals at issue are subject to regulatory screening.

Ivan Harris: Mm-hmm (affirmative). So, in speaking of kind of that innovation, and kind of the new things that are out there, but the old laws apply to them, there still has to be I guess some foundational knowledge for what the current product is; what the latest innovation is, and lawyers are often terrible at doing that. You spoke of the staffing in the Cyber Unit, are there experts that you rely on, or that you're able to call upon to help kind of understand how these things work, and how the novel issues or novel products, or developments that might come your way?

Carolyn W: I just really could not speak more highly about the staff in the Cyber Unit. The staff attorneys there have just put in incredible effort to learn this technology, learn the innovations, and put us in a position to be able to do things like trace digital assets. When you're dealing with the Blockchain, it's public, but there's no account attribution, so you have to figure out how to trace the transactions, and who is the person who owns the wallet, and controls those digital assets. That takes effort. That takes learning tools, learning how to trace these assets, and people have done that, within the Cyber Unit. Similarly, the dark web. It's not as easy to access or search as the traditional lit internet, but there're people who have dedicated their time to learning how to do that, so that they can serve as a resource for the rest of the division. And I think that's something that's very important, and goes to the need for specialized expertise.

Carolyn W: But I will say again, kind of coming back to what I'd said at the beginning, that's something that's not necessarily unique at the SEC. With every case that people have, whether within a unit or not, you have to learn a new industry, or a new company or a corner of the market, and the public servants at the SEC do that, and in the Cyber Unit specifically, it does require the effort of learning these new tools and these new innovations, and that's something that people are very excited to do.

Ivan Harris: So unlike... we've seen for example the Asset Management Unit using industry experts, you haven't seen the need for that in the Cyber Unit; the attorney staff has been able to develop that expertise?

Carolyn W: In those specific examples that I gave, yes. The Cyber Unit does work closely with other specialized units, in particular, the Market Abuse Unit, which is where a lot of the expertise of the Cyber Unit grew out of, and for example, Rob Cohen and a number of us who started in the Cyber Unit had before that been in the Market Abuse Unit, and so on certain cases where the Cyber Unit and Market Abuse Unit work together, for example I think we'll probably talk about the EDGAR hacking case later, and in others, the Cyber Unit draws upon some of the specialists in the Market Abuse Unit, who have that trading expertise, that are quantitative capabilities. They're not lawyers, but they have these skills that nobody else has. And so the Cyber Unit's been able to draw in that.

Ivan Harris: That's great. Great that there's not the siloing that you might sometimes see in other areas. Okay. So, let's move on to speaking of kind of geeking out, my own... kind of the personal history, and the understanding of the way the Commission has worked historically, I thought that the claims that've been asserted and the relief that's been sought in these cyber cases is different, or at least in terms of its concentration then, in other types of cases, in that a lot of the ICO cases are Section Five-only cases: unregistered offering only, without a 10(b) charge, which historically has not been kind of the way the Commission brings what are considered offering fraud cases. And so in these standalone unregistered offering cases, there's usually not, or there's sometimes not disgorgement sought, the relief may be a little bit more narrowly tailored to the type of violation. But it seems that in the ICO cases, the more often than not in the litigated ones, at least, the relief sought is disgorgement, even if there's no fraud charge. And so if you could talk a little bit kind of about the considerations that are going into how to bring these cases? ICOs I guess are a little bit unique, in that oftentimes there's no product, there's no business; there's no... anything, unlike in a typical unregistered offering fraud.

Ivan Harris: So how are you approaching kind of the appropriateness of the relief to be sought, and what can you tell us about some of the thinking within the building about how to seek relief in these cases?

Carolyn W: Sure. So, I think it does depend on the facts and circumstances of each case, and I'm not going to talk about any specific case that's being litigated, but for example, in the settled context we've had some Section Five cases with no disgorgement, as you've mentioned. We've had some that involve a Section Five claim, and have had disgorgement, and so I'll just use those as kind of a way to talk about it. In 2017, we settled with a public issuer called Munchee, which had had an ICO, and they had Section Five charges, but no fraud charges. And according to the SEC's order, after the SEC reached out, Munchee halted its offering, and refunded investor proceeds, before they had delivered any of their tokens, to investors. And in that situation, there was no disgorgement. They

refunded investors. Similarly, just last month, we announced settled Section Five charges against an entity called SimplyVital, that had raised approximately $6.3M in an unregistered sale of securities during a presale. They did it through a SAFT, which people might've heard that term; it's a simple agreement for future tokens, and basically what it meant was that SimplyVital was saying that they would not deliver tokens to investors unless and until they created them. And so the SEC reached out after the presale had started, but before any of the tokens had been generated. And again, in that situation, SimplyVital returned funds to investors that had bought through the SAFTs.

Carolyn W: So again, not a situation for disgorgement. By contrast, in terms of cases where we don't have a fraud charge, TokenLot, which was an unregistered broker-dealer, and also had a Section Five charge, in that case, they settled, and they disgorged approximately $471000. Some of that was derived from commissions they received from profits from selling tokens in secondary markets. But again, a place where we did seek disgorgement. And so I think it depends on the facts and circumstances, and not an exhaustive list, all those caveats, but things that might be considered are how were the proceeds raised? What was done with them? Have they been returned to investors? Those are all potentially relevant factors in terms of what's the appropriate relief?

Ivan Harris: And I get there were two other cases that I think we wanted to talk about, Airfox and Paragon, that seemed to offer a little bit of a hybrid solution, where the issuers were required to offer rescission to investors, but not necessarily disgorge up front the amounts that they had raised. Is that a model that we may see more often, going forward?

Carolyn W: So I don't know that I'd characterize anything as the model, but Airfox and Paragon were important in that they were the first two cases imposing civil penalties solely for Section Five in the ICO registration space. They both conducted their offerings after the Commission's... we refer to it as the DAO Report, in 2017, taking people through how digital assets could be securities. Neither of these offerings qualified for exemptions. But as you said, the settlements had I think two really important parts to the undertakings. One was that Airfox and Paragon had to register their offerings as a class of securities, and file periodic reports with the Commission, which is that investor-protection/giving-investors-information prong that we think is so important. But it also required them to undertake a claims process by which investors could get their money back if they wanted. And so those were our first settlements for violations of Section Five that offered this claims process plus registration, and I think offered a path forward for companies that wanted to comply with the registration provisions.

Ivan Harris: Interesting. Okay. And so then thinking about kind of again some of these novel issues in getting funds back to investors, it's also apparent that fashioning equitable relief in these cases can be a little bit more challenging. In the offering fraud context we're all used to the appointment of a receiver who marshals the

assets, asset freezes at banks, and every penny is frozen. What you've used in these cases is the appointment of an independent intermediary to hold digital assets. Can you give us a little bit of an insight into how that process works?

Carolyn W: Yeah, and I think this is an area where it's required the SEC to adjust, and think about the technology that we're dealing with. So as you said, in a traditional case, if we're worried that assets are going to flee the jurisdiction, or otherwise be dissipated, the SEC can go to court and seek an order, a temporary restraining order or an asset freeze, that then we can serve on banks or brokerage firms, and say, "Keep that money right where it is. Keep those assets right there. Don't let anyone do anything with them." That's difficult when you're dealing with decentralized technology, because that's kind of the entire point: there is nobody in charge, so there's nobody to go to on the Blockchain and say... [crosstalk 00:28:30]

Ivan Harris: "Freeze the Blockchain", yeah-

Carolyn W: "Don't let this money..." [crosstalk 00:28:32] Right.

Ivan Harris: Right.

Carolyn W: It doesn't work that way. And so we've had to think through, well how do we nevertheless protect these assets, as we're dealing with defendants? And so, one of the things the SEC has done is seek court orders that've been granted appointing independent intermediaries, to whom the digital assets have to be transferred. Or a receiver, who takes possession of the digital assets. Again, all with the point of trying to protect them, and make sure the defendants don't have control, and therefore aren't able to dissipate them or transfer them somewhere where we can't reach them.

Ivan Harris: Any other interesting or novel obstacles that you've come across in terms of fashioning the types of relief that we're all used to in your normal case?

Carolyn W: Yeah. So a little bit of a twist on what I was just talking about. Going back to TokenLot, which was an entity that settled, so not a situation where we felt the need to go into court, and try to protect the assets; they've agreed to settle, they've agreed to pay a penalty. But again, just to set the stage, that was an entity where we said they acted as an unregistered broker-dealer. They had in some cases received tokens that they were going to then sell on secondary markets. In some cases they had paid the assets for those tokens but hadn't gotten them yet, and then were going to resell them. So they've agreed to settle with us for handling unregistered securities, in some cases reselling them, and they still have an inventory of some of those securities that we're concerned about. So what do you do in that situation? So the undertakings in the TokenLot order included the appointment of an... they had to go out and retain, sorry, an independent third party, an independent intermediary, to take possession of their inventory. They had to transfer it to this third party, who then destroyed

the tokens, so they could not be resold in the secondary market. Sort of thing you don't always have to think through in that same way, when you're dealing with more traditional forms of securities.

Ivan Harris: I think of taking a hammer to a computer, but I don't know- [crosstalk 00:30:57]

Carolyn W: Doesn't work that way-

Ivan Harris: How else you'd destroy the tokens, but...-

Carolyn W: Yeah. Yeah.

Ivan Harris: Okay.

Carolyn W: The only other thing I'd add in this space is the question of digital asset tracing, which can come up directly in Cyber Unit cases, but it comes up now in lots of different contexts, where people have their assets in something other than traditional fiat currency. And so the SEC, the Division of Enforcement, may be seeking an accounting, or some other way they can verify what those assets are: who has control of them, how much they are, where they are, from defendants, or from people in investigations, because that's what we need to do to figure it out, because we can't just go subpoena a bank, and do it that way.

Ivan Harris: Okay. Last question on this topic, because I'm sure we can talk about ICOs for a while, but there are a couple of other areas that we definitely want to discuss, like a lot of today's illegal activity, it can be conducted from anywhere, and so I'm sure you're seeing a lot of offshore schemes that are being directed towards the United States, or US investors. How is it, the level of cooperation with your non-US counterparts, and are you seeing similar expertise being developed among securities regulators around the world in these types of cases?

Carolyn W: We definitely coordinate and work with law enforcement in international jurisdictions, as well as their securities regulators. They're all very interested in this space; they want to speak to people in the Cyber Unit, whenever they come to visit, or through phone calls. I do think the SEC has led in this area, that the Chairman I believe has spoken about that; that we really saw this problem, and devoted a lot of resources, not just in the Division of Enforcement, but as we've talked about earlier, throughout the Commission. So I think we have a lot to offer to other regulators, and jurisdictions in this space. It is an added wrinkle. It is more difficult when we are dealing with digital assets that on top of that are overseas, or we're dealing with an ICO that has been conducted by people who are all overseas. It doesn't mean we can't do it. It doesn't mean we're not looking into it. But it does present additional challenges.

Ivan Harris: Well, good to see we're leading the way though, at least in those efforts, and good luck in continuing those efforts. So let's move on to cyber security, as the next area of priority that you mentioned. What are some of the biggest risks, I

think, that you're seeing in the area of cyber security today, and in terms of the types of cases, obviously without going into specifics, but the types of things that you're seeing that are causing the unit to start investigations?

Carolyn W: So I mean I think it's fair to say just based on the cases that we've already brought in the last two years, or just looking at the news, that many entities, of all types, face cyber-security risks, face the risk of bad actors trying to access your systems, for a whole variety of reasons, I think one of which is very obvious, and that's that the company, the entity might have a lot of customers and a lot of sensitive personal information, which could be resold on the black market, on the dark web, and so I think that's pretty clear, when you see those reports in the news, of course you understand, "Well I can see why someone would want to get all of that treasure trove of data." Separate and apart from that though, I think there's also the objective of potentially trying to get that information because it might be tradable, and we saw that with the SEC's own EDGAR hacking case, where we alleged that a Ukrainian hacker working with others hacked into the SEC's EDGAR filing system, and obtained test filings of public companies' earnings releases before they had been disseminated publicly, and then traders traded ahead of at least 157 of those announcements, generating over $4M, between May and October of 2016.

Carolyn W: And the hacker and some of the traders were involved in a similar scheme back in 2015 that we charged, to hack into the Newswire services, and get draft press releases there. So I think also looking at entities that might have a large collection of data that could be used to trade is also a concern,

Ivan Harris: So yeah, you have kind of two components of these cases: you have the entities that you might regulate who have the information, and then you have the individuals who hack into that information and maybe can use it for purposes that fall within a securities violation. Let's talk about the former for a second. The Commission obviously I think looks to regulate entities as gatekeepers in this area, and has specific rules in place, Reg S-P, and under Reg S-P the Identity Theft Red Flags Rule, in place to ensure that regulated entities have appropriate policies and procedures. And in last year, in the Voya case, the Commission charged the first violation of the Identity Theft Red Flags Rule, and in the past it has also charged broker-dealers who have been the victims of a hacking scheme, but perhaps did not have sufficient policies and procedures. On the other hand, last year in a 21(a) report, the Commission chose not to charge I think it was eight or nine public companies who had been the subject of business email compromises; the individuals had sent kind of fake emails to get money sent to them, and other types of breaches.

Ivan Harris: So can you tell us kind of how the staff might evaluate whether in that instance to bring a 21(a) report, or to issue a 21(a) report, versus in the Voya and the other hacking-type cases against regulated entities, whether to bring charges against those entities who've been the victims of a hack? How do you go about doing that evaluation?

Carolyn W: Sure. So just for people who might be listening at home like my parents, so a 21(a) report is under section 21(a) of the Exchange Act. It authorizes the Commission to investigate violations of the federal securities laws, and in its discretion, publish information concerning such violations, and contrast that with actually charging violations, which is what you were talking about in the Voya case. So, probably won't surprise you, it depends on the facts and circumstances. A 21(a) report often emphasizes important findings, or is an opportunity for the Commission to provide advice to the public on its thinking, under these areas. And so there've been two very important 21(a) reports in the cyber space. The first one, which I referenced before, we called the DAO Report. That was in July of 2017. And that took on the question of whether a digital asset could be a security. And so it went through the Howey Test that I referenced before, and it cautioned the industry and market participants that just because an entity might be a decentralized organization, just because securities might've been purchased using virtual currencies or might be digital assets, that doesn't mean they can't be a security; and further cautioned the industry, which I think are two additional important points, that market participants handling these digital assets, which are securities, could themselves potentially be liable, and unregistered securities exchanges that provide a trading platform for these securities also could have obligations under the securities laws.

Carolyn W: The second one is the one you just referenced, which was in October 2018, the second 21(a) report from the Commission concerned the question of internal accounting controls that are prone to cyber-related fraud. So that took on the question of the application of internal accounting provisions under the 1934 Act, when what you were dealing with is cyber risks. And so the 21(a) report there dealt with nine companies that, as you said, had been the victim of business email compromises, and each of the nine suffered losses of at least a million dollars, and the nine of them collectively, it was nearly a hundred million dollars, of assets that they had transferred to the perpetrators in response to these fictitious business emails. And so the report explained that public companies need to consider cyber threats, when implementing internal accounting controls. They need to consider the importance of training personnel on the controls, and how to identify cyber incidents. And I think one of the things the report really tried to drive home is that while the cyber-related threats might be new, the obligations under the reporting provisions, the internal controls provisions, those aren't new.

Carolyn W: I would maybe contrast that a little bit with the Voya case that you mentioned, which was a settled matter, and that was under Reg S-P and Reg S-ID, which at a high level require reasonably-designed policies and procedures to protect customer records and information, and against the risks of identity theft. And in the case of Voya, the personally-identifying information of approximately 5600 customers was accessed, and the Commission's order details the failings in the policies and procedures that are required under Reg S-P/Reg S-ID. And so there, you have a situation where there're very specific rules, specifically on cyber

security for a registrant that has the obligation to be protecting customer identity, customer information. And so, we've got that, you've got the 21(a) reports that've now I think provided the guidance and the advice to the industry that when you're putting together your internal controls, you also need to be thinking about cyber-security risks.

Ivan Harris: So is it fair to think of the 21(a) report on the nine companies as, "Here's our guidance. If in a year or two we're still seeing companies fall short on this, we've given you the guidance, we've given you the warning; we may not be as generous next time"?

Carolyn W: I don't think it's fair for me to speak for the Commission on how they might view that, but I think in this space, it is fair to say that there's been the 21(a) report, which I think provides a lot of information, and as I said, it advises the industry on the Commission's thinking. And I think this area is a whole spectrum, and I think we're going to talk about that. But at the other end, you can run into a situation where you've got a company that experiences a very serious data breach, doesn't have the policies and procedures and controls, even though that data goes to the heart of its business, and that's a place where I think the Commission is going to step in and say, "That's just not appropriate."

Ivan Harris: So for the registrants, who maybe are subject to the Reg S-P and S-ID, would self-reporting, would cooperation and remediation, would those be factors in determining whether in this particular instance, maybe enforcement action is not appropriate, versus the cases that've been brought where maybe you didn't see that level of remediation or immediate reaction or cooperation?

Carolyn W: I would say that those are definitely very relevant factors. Whether they are going to carry the day depends on the facts and circumstances of a whole host of things, including the breach; how long it went on, how long you took to tell the Commission, what the remediation has been, what the cooperation has been. But those are things that the Commission and the Division consider, regardless of the context; whether it's cyber or not. We've certainly seen the Commission point to those factors in the cyber space, not specifically in any public way in terms of public companies, but for example, when it comes to registrants, when the Gladius matter last year, in which that was another ICO, another situation where they had not registered the security, Section Five violations but no fraud, but there was no penalty there. It followed after Airfox and Paragon, but no penalty was imposed, and the Commission pointed to the fact that the company self-reported, and then cooperated with the Commission's investigation.

Carolyn W: We also, sometimes the Commission does reduce penalties. So in the case of Zachary Coburn, who was the founder of the digital asset trading platform EtherDelta, there he settled charges for operating an unregistered national securities exchange, and the SEC imposed a $75000 penalty against Mr Coburn, but pointed in the order to the fact that it wasn't higher because of his

cooperation, and including his agreement to testify in any related enforcement action. So I think there are examples of the Commission definitely taking those factors into account in the cyber space.

Ivan Harris: And this may be a little bit more difficult for you to answer, but are there, and again, kind of focusing on I guess the registrants, in this particular instance, are there examples of cases you have not brought, where you looked at the various factors and decided this entity was a victim, had appropriate policies and procedures, or whatever the circumstances might've been, and so we have decided not to bring this case? I know that's difficult, but generally speaking are there any examples you can give?

Carolyn W: Yeah, I just, I can't go into examples of things that aren't public, but I think one thing I can say, and we'll probably continue to talk about this because I know it's a very interesting area, I think we view this as a spectrum. I think we've been very thoughtful in this space. There've been a lot of cyber incidents out there. They're in the news all the time. The SEC hasn't brought that many cases against public companies, for example, for failings with their cyber disclosures. That's not because we're not aware of the incidents; it's because we take very seriously the thoughts that I think have been voiced by the Chairman, by our Co-Directors, that we're not going to engage in second-guessing of reasonable good-faith efforts to disclose cyber-security events, to respond to them, and instead we're going to look at what the facts and circumstances are of the entire situation, and the context.

Ivan Harris: So perhaps an example you could talk about, a well-publicized breach, but we didn't see an action come out of that, but we saw something come out on the second side of the coin, so to speak, that you talked about earlier; Equifax was a victim of a hacking, and the Commission did not bring a case against Equifax, but rather charged insider trading against someone who had knowledge of the hack, and traded on that knowledge before the company disclosed it. So is that perhaps where you're focusing on both sides of the impact of one of these things?

Carolyn W: Yeah, I think the Equifax example, where they had I think it was approximately 143 million customers whose data was breached, is an example of the fact that data breaches and hacking events can themselves create tradable events, for others. And in Equifax, the SEC and there were also parallel criminal charges by the Northern District of Georgia, charged two different individuals at Equifax. The first one was the former Chief Information Officer, and he traded ahead of the company's September 2017 announcement that there had been this data breach. In the SEC's complaint we alleged that he searched the internet, before trading, for the effect on the stock price when one of Equifax's competitors had announced its own data breach, and then within an hour, he had vested his stock options, sold the shares, and avoided losses of $117000. So he was charged with insider trading.

Carolyn W: A couple of months later, we charged a former software engineer at Equifax, who had been tasked with putting together a website for customers impacted by a data breach, and he was told it was for an unnamed potential client, but he figured out it was Equifax, and then he also traded. What he did was he bought put options, so he was betting that the stock price was going to go down. His investment was about $2100. And when the stock price went down after the announcement, he made over $70000. It was more than 3500% return. So he was also charged, by us, and by the criminal authorities. And so I think it just shows that the SEC, as well as the criminal authorities, may have interests in a data breach and a hacking event that go beyond the question of the breach itself, the hack itself; but also whether anybody benefited as a result. And that can include company insiders.

Ivan Harris: So let's continue the discussion then about these public company issues that come up, and the case we've kind of generally mentioned but we haven't talked about specifically, is the 2018 settlement against Altaba, Yahoo!, relating to its massive data breach, and the delay in disclosing it for approximately two years, and the SEC assessed a $35M penalty, in that matter. When the case was brought, Steve Peikin said that, as you pointed out, that although the SEC doesn't seek to second-guess good-faith disclosure decisions, or good-faith exercises of judgment about disclosure, a response can be so lacking that an enforcement action would be warranted. What if anything can you tell us about the Cyber Unit's approach to these types of cases, the disclosure obligations of issuers since then?

Carolyn W: So, I think this is an area that everybody is very, very finely attuned to, and very aware of. The SEC is interested in it, public companies are interested in it. They're interested in it not just because we're interested in it. It goes to their business; they have their own need and interest in protecting data. But at the same time I think we're all very aware that bad actors have a very high level of motivation to keep trying to get this data, so we know that no system is perfect, and that the perpetrators trying to get in are very determined. So the Cyber Unit and I think the rest of the Division takes very seriously this question of how to handle public companies that have experienced a data breach, as reflected in comments, the ones you referenced by Steve Peikin, and our other Co-Director Stephanie Avakian has made similar ones.

Carolyn W: We're not there to second-guess reasonable good-faith decisions, but we need to figure out were they reasonable? Were they taken in good faith? Were the controls that were in place reasonable? And so, I don't think people should be surprised if the SEC has questions after a data breach, trying to understand what's the timeline? When did the breach occur? When did the company become aware? What disclosures if any have they given? What stage are they at trying to figure it out? Were there red flags that were missed? Were there controls that either were never put into place, or weren't enforced? Those are I think very natural questions for the SEC to want to understand, but we're being thoughtful, and trying to put it into context of do we have a situation where a

hack occurred because despite a company's best efforts that's what happened, or do we have a situation where a reasonable person would look at it and say, "No, you know what? That did warrant a different response than what happened here"?

Ivan Harris: And I guess one dilemma that issuers face is they have this disclosure obligation on the one hand, but where a hack has occurred, or some kind of breach has occurred and it has not been disclosed yet, they may be looking to find out who conducted it. They may be working with criminal law enforcement, to investigate the hack, and so they're possibly trying to balance, and disclosure may impede the investigation. Are there mechanisms within the Enforcement Division within the Cyber Unit for an issuer to come in and say, "Look, this happened. We know we have a disclosure obligation, but this is going on. We're working with the FBI, or we're working with this criminal agency, and we just don't feel it would be appropriate to disclose right now"? Are there any mechanisms for that kind of dialogue?

Carolyn W: I would absolutely encourage that dialogue. First of all, I think a long-term strategy of not disclosing an event is probably not a very great one, in this day and age, where you have the media, you have whistleblowers, you might have state disclosure obligations. So kind of hoping that we're not going to find out much less the public is probably not a great long-term strategy. We work with criminal authorities all the time, in all different kinds of cases, most likely the same offices that a company is dealing with, in terms of US Attorney's Office, or the FBI, or somebody else who is helping investigate or look into a data breach, so we're used to dealing with those law-enforcement agencies. The other thing I would say, again, just kind of coming back to, we're not there to second-guess reasonable good-faith disclosure decisions.

Carolyn W: The Commission issued guidance recently on this topic, in February of 2018, and I think there's some really interesting points in there. One is this concept that we recognize that it can take some time to get your arms around what happened; the scope, what was actually taken, who might've been affected, so I think the Commission gets that. But at the same time, the Commission guidance also noted that just the fact that there's an ongoing internal or external investigation, in and of itself, is unlikely to excuse disclosure obligation. So we get that public companies have a lot of competing interests that they're trying to juggle when dealing with something of the magnitude of a cyber-security incident. I think the dialogue with the SEC can help, because at the very least then we're going to know about it, and have an understanding as to what the company is trying to do, to respond to it. And I think the more information we have earlier, the better we're going to be able to understand some of those choices.

Ivan Harris: Okay. Well this has been really terrific. I think unlike a lot of the other specialized units, this specialized unit touches so many different entities and individuals that the SEC regulates, and so whether it's the public companies,

whether it's broker-dealers, whether it's investment advisors, individuals, there're a lot of issues that affect them all, and hopefully all of those entities and individuals have found some of the things you've said to be very helpful, and I think that guidance can be very helpful to them.

Ivan Harris: So, we have completed the hour of this presentation. We thank everyone for being here and participating. We most thank Carolyn for this, and your parents for letting us borrow her for an hour, and with that we'll conclude the presentation. Thank you.

Carolyn W: Thank you very much.