John Wright:

Welcome to Business Better, a podcast designed to help businesses navigate the new normal. I'm your host, John Wright. For nearly 15 years, I was senior vice president and general counsel at Triumph Group, Inc, a global aerospace component supplier. I'm now a member of the securities at M and A Groups at Ballard Spahr, a national law firm with clients across industries and across the country.

John Wright:

On today's episode, we'll be discussing the settlement; the federal trade commission recently announced with Zoom Video Communications, Inc to resolve allegations that Zoom had engaged in unfair and deceptive acts with regard to its video conferencing services. We'll discuss the terms of the settlement, the extensive security measures required of Zoom under those terms, their implications for Zoom and others, and what the settlement suggests may be the focus of future FTC scrutiny. To cover these topics, I'm delighted to be joined by my colleague, Kim Phan, a partner in our Washington DC office. Kim counsels clients across many industries on federal and state privacy, and data security laws, and regulations. Her work in this area includes strategic planning and guidance for companies to incorporate privacy and data security considerations throughout product development, marketing, and implementation, as well as data breach prevention and response. She has also provided guidance to clients on regulatory compliance matters, including investigatory and enforcement interactions with the federal trade commission.

John Wright:

Kim recently blogged on today's topic for Ballard Spars Consumer Finance Monitor blog in a post entitled FTC Zoom Consent Order; Implications for Remote Workforces. You can find a link to Kim's post in this episode, show notes, or on our website. Kim, welcome to Business Better.

Kim Phan:

Thanks John. Glad to be here.

John Wright:

So often with the topics that I'm asked to talk about with some of our colleagues, I have to do a little prep work and I'm unfamiliar with the territory. But, at this point, recording this some nine, 10 months into the pandemic, if there's one thing I feel like I know... And probably everybody in our listening audience knows... It's Zoom. But maybe you could start by telling us a little bit about the background of Zoom, the key facts that we need to know, to set up the discussion we're going to have.

Kim Phan:

Sure. I mean, as you said, I think everyone who will be listening to this is familiar with Zoom video conferencing, and Zoom is a provider of a platform that allows groups to get together via video to meet and collaborate. Zoom offers a variety of free basic services, but also offers a series of monthly and annual subscription plans. And it's interesting, like Xerox and Google before it, since COVID, Zoom has become so ubiquitous. It's now become its own verb. When you say, you have to go Zoom, everyone knows you're going to go to a video meetings. So it's been a big change for that company specifically, as well as for consumers, as well as companies that have to utilize a system like Zoom. And so the security of the Zoom platform is something that has been of great interest over the last few months. It's been heavily criticized in the press. There's been calls by Congress for an investigation, and it response to all

of that, on November 9th, the Federal Trade Commission announced an enforcement action against Zoom related to those security issues.

John Wright:

So what did the Federal Trade Commission alleged in the complaint?

Kim Phan:

So the FTC has authority under its section five of the FTC Act to pursue companies that engage in unfair or deceptive acts or practices. In this case, the FTC actually alleges both. So the FTC alleges that the Zoom was misrepresenting certain information about the level of security it provides. Zoom claim to provide end to end encryption for its meetings. However, the FTC investigation revealed that Zoom actually retains crypto keys that give access to the content of Zoom meetings. So it's not end to end encryption. Zoom also represented that it used 256 bit encryption to secure those meetings, when in reality it was using only 128 bit encryption. Zoom also stated that for paying customers who could record Zoom meetings, that those meeting recordings would be stored encrypted immediately after the meeting ends. While in reality, the FTC discovered that the stored meetings were on Zoom servers for up to 60 days before being transferred to Zoom secure cloud storage.

Kim Phan:

Zoom also allegedly failed to disclose that when it sent out an update to fix a minor bugs for Mac computers running the Zoom platform, that at the same time, Zoom deployed a local hosted web server that circumvented certain Safari browser safe cards that are... Which is the standard browser on a Mac computer. And that that web server had a vulnerability that allowed hackers to download malware to computers. So that wasn't even fixed until as recent as 2019 when Zoom was notified by security researcher that that was an issue. So this is a deceptive practices that the FTC alleged, but the FTC also alleged that Zoom engaged in unfair practices. The installation of that software specifically that was done without adequate notice or consent of consumers, and that the fact that that download would circumvent Safari browser privacy and security safeguards resulted in a situation where consumers were harmed in a way that they couldn't reasonably avoid because they weren't notified of that issue in advance.

John Wright:

Did the FTC make any other comments about Zoom's security?

Kim Phan:

Interestingly, they did. They went into a lengthy analysis of some of the other security failings that they had observed Zoom systems to be deficient in. While these deficiencies did not form the basis for the FTC's consent order, they were laid out in excruciating detail in the complaint. The failure to implement a training program for secure software development, the failure to test its applications for security vulnerabilities, the failure to monitor service providers who had access to the new Zoom network, the failure to use multi-factor authentication, improperly configuring their firewalls, not segmenting their networks or monitoring their systems for hacks, not having an incident response process in place, not mapping their data or inventory or classifying their data, not having a process to delete data, and not having a current security patches. Again, none of these were allegations that formed the basis for the consent order, but were still laid out in detail by the FTC.

John Wright:

Well, all of this sounds pretty extensive and you made some reference to some of the publicity that had occurred well before this was announced. Were those the reasons that these deficiencies were discovered or investigated? Can you tell us a little bit more about how the FTC even got here?

Kim Phan:

Sure. There's been plenty of press about this. A lot of scrutiny from both security researchers, other professionals in the industry calling out some of these failings. There was a lot of political pressure, I think, was also brought to bear on the FTC. There was a number of congressional calls by Senator Sherrod Brown of Ohio; Amy Klobuchar of Minnesota; Michael Bennett of Colorado; Richard Blumenthal Connecticut. As well as on the house side representative Chairman Frank Palone and Jan Schakowsky from the House Energy and Commerce committee. All of them reached out to the FTC saying that this issue needed to be investigated and the FTC need to take some sort of action here.

Kim Phan:

I think there was also pressure, because the FTC was also operating in parallel to some state ag investigation. So attorney generals in both Connecticut and Florida had also announced, publicly and in the press, that they were going to be investigating these issues with Zoom. And I feel like for a certain period of time over the summer, every other week there was another entity that was announcing they were no longer using the Zoom platform due to security issues. For example, the New York City Department of Education actually issued a prohibition against schools in New York City using Zoom for distance learning. So again, a lot of pressure both externally from the public and the media, but also within government from members of Congress to push this forward.

John Wright:

Just to be clear, were there instances of actual access to supposedly secure data that were discovered or learned about in the course of this?

Kim Phan:

Well, I'm sure you've also heard of the new term "Zoom bombing" where someone may penetrate or infiltrate a meeting, and either disrupt it through posting pornography or doing something else that that would be the hacker world innocent fun. As opposed to more malicious activity, someone who was listening in on a financial institution's Zoom meeting, or a healthcare provider's Zoom meeting, and able to collect sensitive information that's being discussed during those meetings. So I think there was a lot of observed issues with Zoom and its security early on before Zoom was able to plug a lot of these holes.

John Wright:

So what changes does the FTC Consent Order require from Zoom?

Kim Phan:

Well the FTC in their Consent Order, it laid out a very comprehensive path forward with how it expects Zoom to operate. The FTC Consent Order is a 20 year consent order that prohibits Zoom from making any further misrepresentations about how it collects, uses, maintains, deletes or discloses information through the platform. But in additionally it requires Zoom to set up a very comprehensive information security program with documented policies and procedures, board level oversight, having a designated

qualified employee named to oversee the program. Zoom's required to conduct annual risk assessments, conduct vulnerability scans on a quarterly basis, capture information in audit logs, require new strong passwords, implement new training for its employees, conduct annual penetration testing, set up a service provider oversight program, including updating its contracts. And then also obtaining independent third party experts to assess its data protection program on a regular basis.

Kim Phan:

Interestingly, the FTC, unlike some of its other consent orders in the past, proactively requires that the company certified the FTC on an annual basis that is in compliance with the consent order. And of course there's some additional reporting and record keeping requirements, as well as the requirement, "Notify the FTC, if Zoom should ever have any future data breaches." So a very extensive consent order.

John Wright:

And it appears to impose many requirements that are unrelated to the specific charges. Is that unusual?

Kim Phan:

So many of these requirements are very typical of FTC Consent Orders, especially in recent years when it comes to various privacy and data security violations. Now there has certainly been criticism brought to bear against the FTC for going above and beyond its statutory authority and imposing these types of requirements. In the few cases where this has actually been litigated, the FTC hasn't always come out on top. For example, in the Lab MD case and in some of the Wyndham Enforcement Actions brought related to data breaches. And it's interesting to note that the FTC actually made some commentary about this in a blog post that is on its website about the settlement. The FTC seemed to feel that it was necessary to justify the need for this enforcement action by stating, and I'll quote, "Even though Zoom has discontinued most of the practices challenged in the complaint, the most effective means for future compliance is a comprehensive security make-over assessed by a qualified third party monitored by the FTC and enforceable in court."

Kim Phan:

So it's interesting the FTC felt the need here. And some of that might be motivated by the FTC's perceived consumer harm that is resulting from these issues with Zoom, because of Zoom's explosive growth right now during COVID. Interestingly, the FTC points out that in December of 2019, there were only 10 million Zoom users, but by April of 2020, just four months later in the wake of COVID, that user number increased to 300 million. So that's a huge increase.

John Wright:

That's astounding.

Kim Phan:

Astounding. Their revenue also exploded, right? So in 2019, their annual revenue for the entire year was about around $622 million. However, in just Q1 of this year, they made half of that, $328 million. Zoom is benefiting greatly, while not also in the FTC's mind, keeping up with where their data security should be.

John Wright:

How unusual is this degree of FTC scrutiny of a tech company's security precautions? Have similar claims been made against other tech companies?

Kim Phan:

Sure. You may have seen earlier this year, Facebook. FTC entered into the largest consent order it's ever entered into with Facebook. It was a $5 billion penalty. That's more than all of the FTC's consent orders combined. So the FTC is very highly focused on technology issues right now, as again, as most folks are working from home or subject to stay at home orders. E-commerce and the ability of consumers to interact online and being fully protected in conducting that activity is something that I think is of a lot of importance to the FTC. And this consent order, while it sounds very stringent, it's not uncommon for the FTC. Say for example, to 20 years. The FTC doesn't have the authority in the first instance to issue civil penalties. Most companies when dealing with the FTC, find that most of the costs related to entering into a consent order with the FTC is the reality of having to comply with the consent order for 20 years. That's the typical length of an FTC consent order. As opposed to-

John Wright:

That was striking to me.

Kim Phan:

It's a long time. In comparison to other agencies, say like the Consumer Financial Protection Bureau who standard consent order is only five years, the FTC... They carry a big stick, we'll say.

John Wright:

So you've already alluded to the fact that in the detailing of the lapses that Zoom was found to have experienced, and then the detail of the remedies that they're supposed to effectuate, there was a considerable amount of detail. Should people looking at that order look at that as an example of what their standards, what the industry standards are expected to be?

Kim Phan:

Absolutely. I think any company that is rolling out or experiencing heavy growth, because of what's happening with COVID, should absolutely be paying close attention to this and implementing parallel data security measures and safeguards to reflect what's happening with this consent order. The reality is that the FTC doesn't have rulemaking authority. I mean, it has requested such authority from Congress multiple times. And while the FTC has issued guidance about what its expectations are for businesses. For example, they have a business guide called Start With Security, that lays out some basic requirements that a small business, per se, might want to implement. The FTC's best and most effective mechanism for laying out the rules of the road of what's expected of companies is via consent order. It's essentially rule-making by enforcement.

John Wright:

So a CIO, or the like, who is looking at road testing their own security systems might be looking at this and similar orders as a checklist for what they might be putting in place, what they should be expected to either have in place, or be able to explain why they don't. Is that fair?

Kim Phan:

That's a fair statement. Some of the challenges with trying to build a program based on consent orders is the uncertainty, right? So if you implement everything that was required of Zoom in this consent order, is that actually enough for your company? The FTC is always very clear in saying that their assessment will be specific to your company, your company size, and the types of products and services that you offer to consumers. So even if you do everything that's required of Zoom, that might not be enough for you. Or if you're unable to implement everything that's being required of Zoom, again, does that constitute an unfair deceptive practice? It's unclear. So it's a very challenging environment for companies to operate in and because the FTC has such broad jurisdiction... The FTC has jurisdiction over every company in America that engages in interstate commerce, except for non-profits and the banks. If you are anyone else, then you are subject to the FTC's authority and would have to be paying close attention to this.

John Wright:

So what's been Zoom's response?

Kim Phan:

Well, Zoom has been pretty clear that they have fixed all of these issues. They think that there's no ongoing security threat. The Zoom consent order doesn't state that Zoom admits any fault here. They have reached an agreement to resolve this issue, but they've been generally silent. There was no press release by Zoom. If you go to their website, they blog about other things, but they don't mention this in particular. I think Zoom is operating business as usual.

John Wright:

And the Zoom bombing hasn't resurfaced?

Kim Phan:

I think that that's still a possibility, right? Even the best security, even under the FTC's standards laid out here, is not 100% security, right? So you could still have a meeting that could be infiltrated, but I think obviously Zoom has done everything they can, everything commercially reasonable within their power to help shore up those issues. Because it's not only an issue of legal compliance, it's also an issue of continued business growth for Zoom. Privacy and data security are absolutely the forefront of consumer's minds, so it has to be at the forefront of company's minds.

John Wright:

So, do we know of any other companies that we think might be susceptible to action like this? Has that been discussed in any respect in the trade press or the like?

Kim Phan:

Sure. I mean, the FTC is frequently in various stages of investigations with various companies. You've probably seen Facebook's a frequent target. The FTC may file, any day now, antitrust charges against Facebook's operations and how they run their business online. I'm sure they're in the process of investigating others. Most of these are non-public investigations until a consent order is announced. So I don't have any inside guidance on that or insights, but I know there's certainly going to be other companies working on this with FTC staff, even as we speak.

John Wright:

So what's been the reaction to the FTC action, either within the industry or otherwise?

Kim Phan:

Well, I think it continues to show that the FTC, while it doesn't have the staffing and resources of some of the larger agencies like the Consumer Financial Protection Bureau, the FTC is still an entity that needs to be contended with. It needs to be treated seriously, and that companies, if they receive a civil investigative demand or even a request for information from the FTC, needs to be treating it seriously. It needs to be considering what their position is, needs to... To the extent that it makes sense for any particular company... reach out to outside counsel that can assist them in navigating working with FTC staff, negotiating with FTC commissioners. There's five FTC commissioners right now, three Democrat. I mean, excuse me, three Republicans, two Democrats. It can be a difficult and challenging process for a company to try to deal with on their own.

John Wright:

I think traditionally, one thinks of the FTC as being one of those that's a little bit more... Bi-partisan might not be the right word... But a balanced so that it may not have a hard shift with the change of administrations, because of the shift in political wins. I don't know whether that's still true today or not, but is any of that reflected in this particular order with respect to Zoom? Did you see anything of that nature that you could comment on?

Kim Phan:

Sure. I think the FTC, like all of Washington DC these days, is becoming increasingly partisan and more stratified in its approach between the Republican and Democratic commissioners. As a five member commission, depending on who is in the White House, three majority commissioners and two minority commissioners. Right now, all five commissioners were appointed by President Trump. So their terms are staggered and they will be slowly rolling off over the next five years. Here in this case, it's interesting, again, the Republicans and Democrats, whereas usually they work together to find a consent order that can be voted on unanimously by the commissioners. Here, the two Democratic commissioners issued dissenting statements. Commissioner Rohit Chopra, who is a Democrat, his term actually has already expired. So he's, I think, holding on until the incoming President Biden can nominate and get the Senate confirmation for a new democratic commissioner.

Kim Phan:

But he criticized the consent order because he believed that Zoom has gotten financial gain from its misconduct and is now in a position of market dominance based on bad acts. And he criticized the consent order because it offered no remediation for effected parties, such as releasing users from contracts who feel like they signed up only because of material deceptive representations. There were no civil penalties entered into against Zoom. There was no admission of fault by Zoom. Specifically he called for the FTC to reinstate a role that has not been filled for some time. A role for an FTC chief technologist who would investigate these types of companies that are high tech and very technology complicated consent orders, rather than simply responding to things like press coverage or calls by the Congress to act.

Kim Phan:

So I think that that is a very different approach from what was actually in the consent order. Rebecca Kelly Slaughter, who's the other Democratic commissioner, she also submitted a dissenting statement and her focus was more that the consent order was very narrowly tailored to issues related to data security. Whereas she would have preferred that the consent order also addressed the related privacy issues that come with these types of failings by an e-commerce platform not to secure the information, being communicated through it.

John Wright:

As we come to wrapping up, I'll ask you to put on your prognosticator's hat and say, as we move into presumably a new administration, do you see anything in this order or in the commissioner's statements that portend something that we can look for in a Biden Administration?

Kim Phan:

Yeah. I think that... What you said earlier is very true. That the structure of the FTC prevents it from experiencing the types of dramatic shifts in direction that some other agencies do. Again, there are currently three Republican commissioners, two Democrat. The next Republican commissioner's term doesn't expire until 2023. So three years from now. While an incoming President Biden could elevate one of the Democrats to the Chairman role at the FTC, which is currently being filled by a Republican commissioner, Joseph Simons, that would change the head of the leadership, but I don't think the five commissioners currently in place are likely to change any time soon. Again, Chopra's term has expired, but he's not about to step down and leave Commissioner Slaughter, the sole Democrat against three Republicans. So I expect him to stay on again until a nominee can be confirmed by the Senate.

Kim Phan:

So not expecting a ton of shift in what's going on at the FTC, as far as their enforcement priorities, as an additional third democratic commissioner rolls on. I think the dissenting statements from Chopra and Slaughter provide a little bit of a preview into what a Democratic controlled FTC might pursue, but the FTC has always been strong in pursuing consent orders in the privacy and data security space. I think we can expect those consent orders to include additional items such as redress or refunds, but the nature of those consent orders, I don't expect it to change that much. But again, the scrutiny is there, the emphasis is there. Privacy and data security is not going away anywhere anytime soon. I expect that to be the same in the next four years under President Biden.

John Wright:

Well, Kim, this has been really interesting and certainly hits close to home for some of us, even though it's the FTC Zoom is an omnipresence. So thank you very much for sharing that with us and joining us on Business Better.

John Wright:

Thanks again to Kim Phan for joining us. Make sure to visit our website, www.BallardSpahr.com, where you can find the latest news and guidance from our attorneys. Subscribe to the show in Apple Podcasts, Google Play Spotify, or your favorite podcast platform. If you have any questions or suggestions for the show, please email podcast@Ballardspahr.com. Stay tuned for a new episode coming soon. Thank you for listening.