

Episode 11- Sanctions & Export Enforcements

Olga Torres: Hello and thank you for joining us today. My name is Olga Torres, and I am the Founder and Managing Member of Torres Trade Law, a national security and international trade law firm. Today is part 2 of a two-part series with David Laufman, a former Chief of the Counterintelligence and Export Control section, “CES,” in the National Security Division of the Department of Justice. Where he supervised the investigation and prosecution of cases affecting national security.

Today we are going to discuss high-profile sanctions and export enforcement cases, DOJ voluntary self-disclosures for violations of the export regulations as well as economic sanctions laws, and the C-suite compliance certifications recently announced by DOJ. At DOJ, David played a key role in the cases against ZTE and Huawei, and is uniquely positioned to comment on current DOJ efforts to promote corporate compliance. We hope you enjoy this episode and I do want to apologize before we get started, for some of you who are maybe wanting to watch our videos. We typically have the audio along with the video, this time we are having a bit of technical difficulties. And rather than postpone the podcast we decided that we would just hold the podcast and transmit via audio only. Having said that we will be available to answer any questions you may have. Typically, during our videos, we have definitions of acronyms, we have links to websites. So, we will try to give you information, as much as we can without using the video. But if not, feel free to contact me or David direct with any questions you may have on any of the discussions, of any of the items we are discussing today. We apologize for the inconvenience, thank you. Welcome David.

David Laufman: Happy to be with you Olga.

Olga Torres: So, let's talk about economic sanctions and export control enforcement and your time at DOJ and, specifically, your involvement in ZTE's case. I mean, as long as you can share it, I'm assuming there's some things you cannot share, but.

David Laufman: Sure. Well, enforcement of U.S. export control and sanctions laws was a major responsibility that CES had. CES is part of the National Security Division and the enforcement of the U.S. export control and sanctions laws is a major national security priority for the Department of Justice as part of the law enforcement community with Commerce and State Defense Directorate of Trade

Controls and OFAC. And the ZTE case along with the early phases of the Huawei case were probably the most significant cases I oversaw. I think the Schlumberger case preceded ZTE. But in ZTE we were confronted with a major Chinese company – I think one of the top two manufacturers of telecommunications in China, championed by the Chinese government – and the government's investigation determined that ZTE had willfully violated U.S. export control and sanctions laws by shipping items to Iran containing U.S.-origin goods. That would have been bad enough, but it was ZTE's conduct during the course of the ensuing investigation which really magnified the egregiousness of ZTE's conduct and criminal liability because it was quite brazen. As the public record indicates they lied about having stopped shipping U.S. origin goods to Iran, they lied to the U.S. government about that. They lied to their own lawyers about that worse.

Olga Torres: I remember, I remember that.

David Laufman: I think highly of their outside counsel at the time. I'll never forget getting a phone call from their outside counsel when I was visiting my grandchildren in Nashville to report what she had learned, to her horror, about her client's behavior which he brought to our attention.

Olga Torres: That must be a very stressful call for that counsel.

David Laufman: Can you imagine? I'll never forget. That became fodder for additional charges that they had to eat in their criminal prosecution. They also hid from the very consulting firm retained by outside counsel to audit their compliance. They hid evidence of non-compliance. They hid evidence of violations by altering data in the system made available to the consulting firm retained by outside counsel, and that also featured in their criminal prosecution. And they were also supposed to jettison, meaning they were supposed to fire, anybody in the company that had been associated with these violations and they committed to doing that. And as it turned out, as evidenced by a second monitor that the Commerce Department imposed on them, they lied about that too.

Olga Torres: Yes

David Laufman: This is the first company in history, whether Chinese or not Chinese, I think that has ever had two compliance monitors foisted on them. It's a cautionary tale in a couple of respects. One, to see, despite the best due diligence that outside counsel may bring to bear and really engaging in customary due

diligence with our clients to make sure they've been candid with us and sharing all the relevant facts that things happen sometimes where clients are not completely candid with us. This would not be news to someone who's ever represented someone, in a criminal prosecution. But for expert control and sanctions lawyers, I think it's a little more novel. So, there was that feature of it just, how much more can we do as lawyers to make sure that our clients are telling us the truth. Especially when we are relaying what we hear from our clients to law enforcement.

Olga Torres: And especially when you have auditors involved, right? I mean, then you have the audit to at least uncover, but they're also lying to the auditor. So, yeah, that's crazy.

David Laufman: It's really quite extraordinary fact pattern then. Then at the end of the day, when we finally were at the altar in federal district court in Dallas, after a very difficult investigation and rather complex negotiation to result in the plea. Where we had gone through meticulously and professionally our consideration of what monitors we believed would be appropriate. The federal judge overseeing the plea, pulled the rug out from us at the 11th hour and installed somebody to service the monitor in the first criminal case who had zero, I underscore, zero experience in export control or sanctions matters. In this case, the court took the matter out of the hands of the parties and their own understandings and agreements and installed a monitor that's now been an operation for years and that I'm, I hear has billed in the tens of millions of dollars.

There are incentives for companies to cooperate. Some of those incentives are expressed in some concrete terms in voluntary self-disclosure policy guides that the Department has issued. The first version of that we put out under my watch, I think in 2016. It's been refined and made more explicit, I think, in 2019. But the whole goal is to bring about cooperation through providing all relevant information about all violations, including violations by individuals in the company who caused the violations on the premise that companies are inanimate things and only humans that run them can actually engage in criminal behavior.

In my experience, it is unusual, particularly in the area of export control and sanctions areas for a monitor to be installed with zero substantive expertise. This is complicated stuff, right, Olga? It's complicated.

Olga Torres: Right, it's very technical.

David Laufman: It's very technical in nature. And enormous inefficiencies created by installing a monitor with zero substantive experience. It makes no sense and it's unfair. I mean, there have been times I hasten to pause where I have almost felt empathy for ZTE over the years, knowing what this monitor has put them through. And it's just, to me, it's a stigma associated with the latter stages of that enforcement matter having to do with how the court behaved and has gone along with this. There's practically nothing more onerous as you know, than a company having to be subject to a compliance monitor for some period of years. It's enormously costly and sometimes it's necessary because the alternative facing criminal prosecution can bring about even more damage, especially reputationally. But that's what hangs in the balance.

Olga Torres: Very interesting. Well, companies: don't do that, do not conceal. Do not do anything that will get you in a situation where you're dealing with DOJ and on top of it with a monitor. My next question is a good follow up to that. We always had the mechanisms, the voluntary self-disclosures with the DDTC Director of Defense Trade Controls and the equivalent with Department of Commerce, Bureau of Industry and Security, or Office of Export Enforcement. It was not until fairly recently when DOJ had guidance on a DOJ equivalent for, specifically, violations of export and economic sanctions law. But my question there, it is actually really interesting, I remember when it first came out there was a little bit of, I don't know what the term would be, sarcasm, of whether people would actually submit a voluntary self-disclosure where you would actually have to say that there was knowledge, that there was intent. Right? It just seems like such a scary because remember a voluntary self-disclosure is nothing short of a confession. So, how do you think, are companies using it?

Can you talk about the benefits from a DOJ perspective? Can you remind us what the guidelines were and I believe they were recently amended. Can you just give us background on that and whether companies that suspect knowledge violations, whether it would be wise for them to submit, not just to let's say OFAC or DDTC or BIS, but also to DOJ?

David Laufman: Sure. Well, the voluntary self-disclosure policy regarding export control and sanctions was first issued in October 2016 when I was serving as Chief. And it was intended to be modeled on, not identical to, but modeled on the Criminal Division's voluntary self-disclosure policy for violations of the Foreign Corrupt Practices Act. And we loosely modeled it on the FCPA policy. It was not as quantitative in its recitation of benefits. I think what evolved was a recognition

over the next three years that the policy needed to be more explicit about what the benefits would be. Making more concrete what those benefits would be. And so, that as a result, I think they assessed, they needed to issue a revised policy. That's what they did about three years later in December of 2019. This policy offers a non-prosecution agreement to companies that submit a VSD, and the possibility of not having to pay a fine where there are not aggravating factors. And aggravating factors take on a broad waterfront of criteria, where the efforts to conceal how egregious was the conduct, the more evidence that willfulness there was, the more aggravating the conduct is likely to be found. But even if there are aggravating factors where there is complete cooperation and timely disclosure, and that encompasses a lot in those terms too, a company can still qualify for a 50% reduction in fine and can not have to endure the slings and arrows of misfortune, of being subject to a monitor if they have instituted a strong compliance program.

So, it's a big deal for a company to agree publicly to having violated U.S. export control and sanctions laws. And some companies have to make an assessment of the degree to which their conduct will come to light. There is reputational harm as well as financial harm to the company by admitting to potential criminal violations, individuals lose their jobs at companies like this, stock value can sometimes be impacted, and then of course there's always the risk that they will have to be subject to a monitor. And as we saw in this ZTE case, these things can take on a life of their own over a period of years and cost them tens of millions of dollars.

Olga Torres: Yeah. In terms of the timing, and this may be more in the weeds, but a quick question that I just thought of. For example, if there's a company that is submitting an ITAR VSD, and it's not right away apparent that there could be some knowledge, right? I mean, sometimes you don't see this until much later in investigations. If, for example, there was already a referral by the civil agency, by OFAC or DDTC to DOJ. Are you barred at that point from submitting a DOJ VSD? Like at what point are you?

David Laufman: No. There's actually even a footnote in this policy that makes clear that companies may not know all the relevant facts at a time where they may make a disclosure to a regulatory agency. What the Department is aiming for is to have disclosures made simultaneously to the Justice Department, as well as a regulatory enforcement agency, like BIS at Commerce or, DDTC. But they understand sometimes that companies will not learn until later that conduct perhaps should have been disclosed to the Department of Justice as well.

So, what the policy is intended to reward is disclosures where the party disclosing that became aware of an ongoing non-public investigation, that's where the company will be considered to have made a voluntary self-disclosure. If the Department has learned about it already, then they're less likely to get voluntary cooperation credit.

Olga Torres: And that will be in a situation where there's already a referral, right? By let's say Department of Commerce to DOJ?

David Laufman: Right.

Olga Torres: Lately a lot of what we hear and read is the sanctions against Russia. And DOJ stated, I believe it was at a conference that “sanctions are the new FCPA.” I wanted your comments on that statement and also just generally the use of monitorships in new cases by DOJ. And your thoughts on that?

David Laufman: Well, as you well know, from your sanctions practice, Olga. The sanctions compliance business has taken off into orbit since the Russian invasion of Ukraine. Advising clients on how to steer clear of business engagements that may otherwise require a license or be prohibited under executive orders has become a whole cottage industry in and of itself. I think it's a misnomer to say that we're suddenly seeing real sanctions enforcement for the first time, simply because of the Russian invasion of Ukraine, but it has certainly gone to a new level. I don't think we've begun to see the tip of the iceberg of potential criminal prosecutions that may ensue. It takes time for criminal investigations to catch up to new sanctions regimes. But I think we've already begun to see some of that. I think we'll see a lot more of it. It took time when the first Iran sanctions went into effect before we began to see criminal prosecutions. It takes time to build criminal investigations. I think we're likely to see a surge of public facing criminal enforcement action with respect to the mosaic of sanctions that have been instituted now regarding Russia's invasion of Ukraine.

Olga Torres: I know I said I wouldn't ask you any other questions, but I just thought of something: What are your thoughts on DOJ's new policy with respect to corporate resolutions, where they're asking for DPA, deferred prosecution agreements, and non-prosecution agreements are requiring, or they will require, the CEOs and the COOs to certify that the compliance program is a good compliance program. What are your thoughts on that? I know people were nervous about that.

David Laufman: Well, from my current seat, which is no longer on the enforcement side, I think it's I think it's problematic. It's really raising the cost, isn't it to the people, first of all, to take those compliance jobs, because I would be wondering whether I'm putting my own liberty on the line to have to certify things that I may not have a hundred percent confidence in. Compliance officers, senior corporate officials who seek to push down a culture of compliance often, despite their best efforts, can't bring about a hundred percent compliance. You don't know what you don't know. So I think there would be a certain amount of angst that would accompany those certifications even after enormously invasive internal investigations that may take place, because you just can't be a hundred percent sure. So, who would want to sign their name to something going to the Department of Justice? Unless you had metaphysical certitude of what you were saying was true.

Olga Torres: Yeah, even after you have excellent compliance programs, things can go south, right? Or you can have an employee acting solo or maybe something that you didn't foresee when you implemented the compliance program, especially for very large corporations. So, I agree with you, but...

David Laufman: I mean, I think as a practical matter if an enforcement investigation arose where questions were raised about whether a certifying chief compliance officer made false representations to the government. The record will be what the record will be. In many cases I'm sure it would be something that the compliance officer in fact did not know was happening when they certified. But that's going to cause a long period of uncertainty and anxiety for that compliance officer.

Olga Torres: Well, we'll see if that increases awareness and maybe gets people a little more resources which I'm sure is what the DOJ wants. Thank you so much for your time today and thank you to our listeners for tuning in. We'll bring you more of timely topics on trade and national security next week. Thank you.

David Laufman: Thank you very much. Good to be with you.