

INSIGHTS

## Know Your Client, Know Your Customer, Know Your Counterparty Practice

March 23, 2022

By: [Matthew G. Nielsen](#) and [Seth D. DuCharme](#)

On this episode of The Bracewell Sidebar, [Matthew Nielsen](#) talks with our new podcast co-host, [Seth DuCharme](#), about developments in white-collar enforcement, including the recent sanctions against Russia and the aggressive enforcement positions being taken by various agencies.

**Let our listeners hear your thoughts on what you expect in the world of white-collar enforcement over the next year, year and a half.**

I think the main takeaway from what we've seen over the last year, right up until the last few days, is an increasing requirement for corporations and individuals to invest more time and energy in the know your client, know your customer, know your counterparty practice.

The administration and the executive agencies within the administration have been pretty coherent and consistent from very early on in the messaging. We've followed these developments in some of our client alerts and certainly some of our internal conversations and conversations with our clients. The administration came out pretty hard and pretty early that a focus was going to be on international corruption, on energizing white-collar enforcement, whether it was through FCPA enforcement by the justice department or aggressive regulation by a number of agencies. Cryptocurrency, of course, is the fuel that flows through a lot of the transactions that are under review, and the creation of a number of different task forces out of DC.

This sort of goes back to the spring. We were seeing one after another a White House memo on any corruption and a new task force. Then into the fall, of course, at the White-Collar Conference in Miami, the deputy attorney general turned heads, I think it's fair to say, with a very aggressive announcement about how the department was going to revisit some of its prior policies and practices on such things as monitorships and the exercise of discretion to open investigations into corporate conduct. That had a lot of us in the white-collar bar talking in the fall about how is this going to manifest.

**Sometimes enforcement priorities tend to be reactive, rather than proactive, such as the aggressive sanctions and some of the unprecedented sanctions that have been issued against Russia. The United States is going to be looking to bring enforcement actions relating to that. They almost have to, to put some teeth behind those sanctions.**

This year's Meet the Regulators panel at the White-Collar Conference included the current director of enforcement for the Commerce Department. The Commerce Department has a team of agents nationally that focus on investigating and enforcing the International Emergency Economic Powers Act, which is the criminal statute that relates to the sanctions regime that Treasury implements and that the executive orders stand up. Not only did you have the AG saying broadly, "You're going to see a lot of white-collar investigation enforcement. We're going to focus on individuals," but you had the head of enforcement from commerce talking about control technologies, exports, and this was even before the sanctions really started flowing from the White House and Treasury.

So, you've got an aggressive Commerce Department looking to make a name for itself. You've got all these DOJ task forces, the Kleptocracy Task Force, and the president in the State of the Union saying they were going to be going after the assets of oligarchs. So, it's not just Treasury and DOJ and Commerce. You've also got the State Department, which controls the export of things on the munitions list and the material of war that's broader than most folks realize. The overlap of sanctions enforcement with the appetite to make white-collar cases is going to result in some civil action, and possibly even some criminal action, for those foolish enough to bury their head in the sand with respect to who they're dealing with and what they're trading in.

**So, it's really important to know who you're doing business with. As for the companies that are selling controlled technology, hopefully they have a mature program in place to help make sure that they're not selling things where or to whom they shouldn't be.**

We also have to harden the target a little bit in terms of retaliation or the vindictiveness of the Russian government and those who are aligned with it.

The perfect storm that we have now is that potentially you've got a Russian economy that we are effectively starving of money and goods and any technology that could fuel the war machine. That's a lot of stuff, and the Russian government is a tier one foreign state actor with a lot of capability to create shell corporations, to engage in cyber activity. It has assets all around the world. In a digital world, doing KYC to the point where you can penetrate all the layers of backstop for an individual or a corporation to give you comfort that you're not accidentally doing business with a witting Russian asset, is going to be challenging.

Have questions? Send your emails to [Matthew Nielsen](#) or [Seth DuCharme](#).

*The opinions expressed in this podcast are those of the speakers and do not necessarily reflect the viewpoint of their institutions or clients.*