BRACEWELL

INSIGHTS

The Crossroads of Crypto and Cyber

June 29, 2022

*By: **Seth D. DuCharme***

On this episode of Bracewell Crypto Bits, Anne Termine is joined by New York partner ***Seth DuCharme*** for a discussion about the intersection of cryptocurrency and cybersecurity.

Prior to joining Bracewell in 2021, Seth served as principal associate deputy attorney general of the United States and the acting US attorney for the Eastern District of New York. While at the Eastern District, he held several positions, including Chief of the National Security and Cyber Crime Section.

Highlights

There has been so much happening in crypto and cyber over the last several months. The scrutiny of crypto businesses with respect to a focus on customer investor protection has been a key talking point for almost every regulator out there. Can you tell me a little bit of where crypto and cyber come together?

I find that the terms "cyber" and "crypto" have probably reached a point of diminishing returns in their usefulness, because so many things fall under the heading of "cyber," and frankly, the same can be said for "cryptocurrencies." The problem there is that you can have a wide divergence of expectations across people who think they're talking about one thing when the other side is really talking about something else.

Cyber and crypto used to be exotic to some degree. When I helped stand up the Cyber Crime Section, the first Cyber Crime Section that we had in the US Attorney's Office in New York, we were trying 10, 12 years ago to figure out what that was really going to be in terms of a federal criminal practice. What is the intersection between essentially a computer and criminal activity? As you know, there's a lot.

Cryptocurrency also still has a little bit of the air of the exotic, but both cybersecurity and cyber instrumentality, and also cryptocurrencies, are not quite to the point of kitchen table conversation in every household in America, but they've come a long way in that direction.

You recently wrote an article about the Office of Foreign Asset Controls (OFAC) conference and in it discussed the whole-of-government approach to cybersecurity, the Bank Secrecy Act, to anti-money laundering and know-your-customer. What is OFAC, and why is OFAC focused on crypto?

OFAC is part of the Treasury Department. It has a lot of discretion to list individuals and entities with whom one cannot do business, essentially if one is a US person within the definition of the regulations.

OFAC is an interesting creature because its power largely is derived from executive order, and the purpose behind the scheme is to give the president (the chief executive), the ability to move quickly and nimbly to respond to national security and economic crises facing the United States.

For folks who were in the middle of transactions that were legal yesterday and illegal today, or in a few months per the wind down period, the main purpose behind OFAC sanctions is to promote the national security and economic health of the United States. For foreign policy and domestic protection, OFAC can rely on classified information, which they do not have to share in making these essentially national security decisions.

The word "sanctions" and the agency of fact became almost a daily conversation with the Russian war on Ukraine and within that, there was a lot of froth about crypto and crypto companies maybe being used to evade those sanctions. What actually has played out since then?

The use of cryptocurrencies to facilitate transactions, both innocuous and nefarious, is something that is evolving, and we collectively, both the United States government and the firms that advise clients, are collecting information. To answer your question directly, my understanding is cryptocurrency, like any other instrumentality of wealth, any other tool of wealth transfer, can be used both for money laundering and sanctions evasion. The challenge for, let's say, the government of Russia or Russian entities under the Russian sanctions, is that there's really likely not enough cryptocurrency in the market right now. For someone who's got really significant wealth — billions with a B — to try to move that wealth around undetected by regulators or the compliance departments of well-meaning corporations, because you'd have to basically accumulate all of it, that would look pretty suspicious.

If there's one takeaway from the perspective of OFAC and sanctions for crypto companies, what would it be?

Clients and law firms need to match the tempo of the evolving sanctions situation. This is a much faster tempo than many folks are used to. Other types of legislation move slowly; sanctions move very quickly. Again, not to be a fear monger, but somebody needs to be paying attention on your behalf to OFAC's near daily announcements of who's been added to a sanctions list or what directives or general licenses have been issued, so that you can spot in real time where liability exposure, whether legal, commercial or reputational may be attaching to a deal that you're working on or a matter that you're involved in. Then just think holistically. If an entity's being sanctioned, that's a pretty good indicator that there are other areas of potential exposure around that entity that could incur other types of civil or criminal liability in the US system. Unfortunately, this is one where you have to pay attention every day or delegate that to somebody else.

Have questions about issues related to cryptocurrency and cybersecurity? Email ***Anne Termine*** and ***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.