Practical Issues in Cyber-Related Sanctions

GIR: The Guide to Sanctions - Second Edition
07.13.2021

We are pleased to announce that Brian Fleming, Timothy O'Toole, Caroline Watson, Manuel Levitt, and Mary Mikhaeel authored the "Practical Issues in Cyber-Related Sanctions" chapter in the second edition of *Global Investigations Review*'s *Guide to Sanctions*. "The United States has been at the forefront of establishing a cyber-focused economic sanctions regime, which is primarily administered by the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), although criminal prosecutions for certain willful sanctions violations are the responsibility of the U.S. Department of Justice," the authors wrote. "OFAC administers a variety of sanctions targeting malicious cyber-related activities, such as cyberespionage, cyber-intrusions on critical infrastructure and computer networks, and disinformation campaigns conducted from abroad. The bulk of these sanctions are administered under OFAC's 'Cyber-Related Sanctions Program', which was established in 2015 as part of the Obama administration's response to malicious cyber-enabled activities originating from foreign countries that were directed at both U.S. government agencies and private sector U.S. entities. However, sanctions targeting malicious cyber-related activities are also authorized under other statutory and executive branch sanctions authorities, including the Countering America's Adversaries Through Sanctions Act (CAATSA), as well as Executive Order (EO) 14024, Blocking Property With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation, issued on April 15, 2021."

In the chapter, Brian Fleming, Timothy O'Toole, Caroline Watson, Manuel Levitt, and Mary Mikhaeel review the development of U.S. cyber-related sanctions regimes. The authors discuss cyber-related compliance risks and provide practical considerations to mitigate cyber-related sanctions compliance risks. They conclude by highlighting strong incentives the U.S. government enforcers provide in exchange for voluntary disclosure and robust cooperation by companies that have committed potential U.S. sanctions violations, which apply equally in the cyber context.