Trade Compliance Flash: Leading Chinese Telecommunication Provider Huawei Technologies Indicted in Two Separate Cases

International Alert
02.01.2019

On January 28, 2019, the U.S. government announced two separate criminal indictments against Chinese telecoms equipment provider Huawei Technologies Co., Ltd. (Huawei), three of its subsidiaries, its CFO, and other unnamed individuals. The first indictment, brought in the Eastern District of New York (EDNY), focuses on alleged violations by Huawei and its subsidiaries of the current U.S. sanctions on Iran, as well as related conspiracy, bank fraud, wire fraud, and money laundering charges. The second, brought in the Western District of Washington (WDWA), focuses on Huawei's alleged attempts to steal trade secrets from a rival U.S. telecommunications company, T-Mobile USA (T-Mobile).

Due to Huawei's role as a leading light of China's emerging high-tech sector and alleged connections to the Chinese military, the indictments are likely to complicate the ongoing trade negotiations between Beijing and Washington. The indictments are also part of a broader trend of economic sanctions and export control enforcement in the Asia Pacific region.

Our summary and analysis of the indictments are set forth below.

EDNY Indictment for Iran Sanctions Violations, Wire Fraud, Money Laundering, and Obstruction

The U.S. Department of Justice's (DOJ's) indictment in the EDNY alleges violations of the Iran sanctions, as well as bank fraud, wire fraud, conspiracy to launder money, and obstruction of justice. In addition to the Shenzhen, China-based Huawei, the indictment also charges the company's CFO Meng Wanzhou, U.S. subsidiary Huawei Device USA, Inc., and alleged Hong Kong-registered subsidiary Skycom Tech Co. Ltd. (Skycom), also allegedly a subsidiary of Huawei.

Most of the indictment focuses on alleged conspiracy, bank fraud, wire fraud, and obstruction of justice charges arising out of Huawei's efforts to conceal its Iran business from U.S. authorities and financial institutions. Specifically, Huawei allegedly lied to financial institutions and U.S. government authorities concerning this relationship and its business in Iran, providing false information to financial institutions and the U.S. Congress, and made false statements to agents from the Federal Bureau of Investigation (FBI) investigating the company. Additionally, when Huawei learned of the government's investigation, it allegedly tried to move potential witnesses outside of U.S. jurisdiction, as well as conceal or destroy any evidence located in the United States.

The indictment also includes charges that Huawei and its subsidiaries sought to circumvent the Iranian Transactions and Sanctions Regulations (ITSR). The indictment provides fewer factual details to support these allegations, but they appear to center around Huawei's use of its "hidden" or "unofficial" Hong Kong subsidiary Skycom to obtain U.S.-origin goods, technology, and services (including financial services) that could subsequently be provided in support of Huawei's business in Iran.

The indictment also includes charges against Huwaei CFO Meng Wanzhou, who was arrested in Canada in December 2018 and is currently fighting extradition to the United States. The indictment alleges that Meng played a personal role in defrauding U.S. financial institutions in a scheme to evade U.S. sanctions on Iran, particularly in a presentation she made to a major banking

partner in which she denied Huawei's relationship with Skycom and misrepresented Huawei's compliance with U.S. sanctions and export laws. Finally, the indictment appears to charge individuals whose names have been redacted, presumably because they have not yet been apprehended or are cooperating with the U.S. government's investigation.

WDWA Indictment for Theft of Trade Secrets, Wire Fraud, and Obstruction

The WDWA indictment alleges conspiracy to commit theft of trade secrets, attempted theft of trade secrets, and related counts of wire fraud and obstruction of justice. The trade secret theft charges arose out of an alleged scheme to steal a proprietary technology used in a robotic phone testing system nicknamed "Tappy," which was developed and operated by T-Mobile, a partial U.S. subsidiary of the German telecommunications giant Deutsche Telekom.

According to the indictment, while Huawei was developing its own phone-testing robot called "xDeviceRobot," company personnel instructed their colleagues working with T-Mobile under a separate supply agreement to collect as much information as possible about Tappy, including by requesting photographs, collecting detailed technical specifications, and asking T-Mobile employees specific questions about the robot's functioning.

Huawei claimed in later litigation with T-Mobile that such efforts to obtain Tappy's technology constituted an "isolated … moment of indiscretion" contrary to company policy. However, the indictment alleges that Huawei's China-based subsidiary had issued a formal bonus program for employees who stole confidential information from competitors, indicating a culture supporting trade secret theft.

Huawei's use of e-mail in support of the alleged trade theft scheme constituted the basis for the wire fraud charges. The indictment also alleges that Huawei obstructed justice during civil litigation with T-Mobile, as well as during separate grand jury proceedings.

Noteworthy Aspects

- **The Reach of U.S. Jurisdiction**. The EDNY indictment emphasize U.S. authorities' broad interpretation of the jurisdictional reach of the United States, particularly with regard to economic sanctions targeting countries like Iran. Notably, as non-U.S. persons, the Shenzhen- and Hong Kong-registered companies Huawei and Skycom may not have technically been subject to the Iran sanctions set forth in the ITSR. They therefore may have been able to conduct some business in Iran – so long the business involved no U.S. persons, goods, services, or technology. However, by allegedly engaging in a scheme to route U.S.-origin goods, technology, and services to Iran and employing at least one U.S. citizen in Iran, Huawei and Skycom may have *both* subjected themselves to U.S. jurisdiction *and* violated the ITSR simultaneously. For this reason, it is crucial that non-U.S. companies understand the potential bases for U.S. jurisdiction – including U.S. subsidiaries, employees who are U.S. citizens, U.S.-origin technology, and U.S. dollar transactions – as well as how to comply with applicable economic sanctions and export controls.
- **The Coverup Can Be Worse Than the Crime**. Some charges brought in both the EDNY and WDWA indictments focus on Huawei's alleged efforts to conceal its underlying criminal conduct. In fact, the majority of the EDNY charges are bank fraud, wire fraud, or obstruction of justice, and Huawei CFO Meng Wanzhou's potential personal criminal liability appears to be entirely based on her alleged role in concealing the company's Iran business. Bank fraud, wire fraud, and money laundering charges are a common tactic that U.S. authorities use to enforce U.S. economic sanctions, export controls, and even anti-corruption law. This tactic allows multiple charges against a single defendant – strengthening the government's hand for trial or plea negotiations – and often allows prosecutors to more easily prove their case based on easily obtainable evidence such as emails, documents, and, in the case of Meng Wanzhou, PowerPoint presentations.
- **DOJ's Focus on China**. The indictments against Huawei appear to be a part of a larger DOJ enforcement crackdown focusing on China. Notably, in 2018, the U.S. government brought enforcement actions against a number of high-profile Chinese companies for alleged sanctions and export control violations – including ZTE Corporation, Fujian Jinhua Integrated Circuit, and Yantai Jereh Oilfield Services Group – and brought criminal charges against several Chinese companies and individuals alleged to

have willfully provided sensitive technologies to China. Furthermore, in November 2018, then-Attorney General Jeff Sessions announced a new "China Initiative," a legal and prosecutorial strategy that ties together U.S. objectives connected with intellectual property, international trade, anti-corruption, and national security. Based on these and other indictments, we expect Chinese companies and individuals to continue to face high enforcement risk for the foreseeable future.

For more information, please contact:

Brian J. Fleming, bfleming@milchev.com, 202-626-5871

Timothy P. O'Toole, totoole@milchev.com, 202-626-5552

Aiysha S. Hussain, ahussain@milchev.com, 202-626-1497

Collmann Griffin, cgriffin@milchev.com, 202-626-5836

Caroline J. Watson, cwatson@milchev.com, 202-626-6083
