U.S. Government to Heighten Enforcement Efforts and Seek Private-Sector Cooperation against Chinese Technology Theft; Spike in Charges Against Companies and Individuals Expected

On February 6, 2020, senior government members—including the heads of the U.S. Department of Justice, Federal Bureau of Investigation, and National Counterintelligence and Security Center—as well as Main Justice and line prosecutors, attended and spoke at the China Initiative Conference, hosted in Washington D.C. by foreign policy think tank the Center for Strategic & International Studies. Discussions at the conference provided key insights into the U.S. Government's law enforcement priorities for the coming year under the Department of Justice's China Initiative, which was launched in November 2018 to address threats posed by Chinese efforts to seize and control technologies that are anticipated to shape the future of economic growth. Attorney General William Barr, who delivered keynote remarks, along with FBI Director Christopher Wray, emphasized the need for cooperation from industry and academia in dealing with the challenge. The head of Main Justice's Criminal Division as well as line prosecutors from New York, Boston, Texas, and Alabama advised that a spike in charges can also be expected against companies and individuals suspected of stealing U.S. technology throughout the coming year.

I. The China Initiative

In November 2018, the Department of Justice launched the China Initiative with the following stated goals:

- identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law;
- develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
- educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;
- apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate;
- equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;
- implement the Foreign Investment Risk Review Modernization Act for the Department of Justice (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
- identify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks;
- identify Foreign Corrupt Practices Act cases involving Chinese companies that compete with American businesses;
- increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement with the United States; and
- evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

II. Key Takeaways from the China Initiative Conference

Specifically regarding enforcement efforts against hackers, Attorney General Barr, FBI Director Wray, and U.S. Attorney / Department of Justice Criminal Division representatives emphasized that:

- The Department of Justice's indictment of 10 hackers in December 2018 outlined a global campaign, associated with the Chinese Ministry of State Security, targeting IP and confidential business and technology information belonging to hundreds of clients of managed service providers worldwide.
- The U.S. Government will use a host of tools, from criminal charges and civil injunctions to economic sanctions, entity listings, and visa revocations. Law enforcement agencies are also working with CFIUS—the Committee on Foreign Investment in the United States—in its review of foreign investments in American companies that produce critical technologies or collect sensitive personal data of U.S. citizens.
- Eastern District of New York U.S. Attorney Richard Donoghue expected "some very interesting prosecutions coming forward" as prosecutors start going after businesses.
- Massachusetts U.S. Attorney Andrew Lelling, responsible for Boston, also predicted a spike, but said that he believes the number of cases he prosecutes should fall after academic institutions in the area start shielding themselves better against the threat.
- Northern District of Alabama U.S. Attorney Jay Town noted that he would like to see the Foreign Agent Registration Act, which requires agents of a foreign government who are in the United States in a political capacity to let the U.S. Government know, be expanded to include people sent by a foreign government for research and development purposes.
- The U.S. Government also seeks a whole-of-society response, with government and the private sector working together. Intelligence and law enforcement communities are working harder to give companies and universities the information they need to make informed decisions and protect their information assets. In return they seek careful decisions by executive and boards of directors regarding whom they do business with or make part of their supply chain, and encourage universities to seek transparency and reciprocity in agreements with foreign institutions plus to perform due diligence on foreign nationals who seek to work or study on their campuses. The U.S. Government also asks industry and academic partners to reach out to them if they see anything concerning.

III. Follow-On Prosecution Announcement

On February 10, shortly after the conference, the Department of Justice announced indictments by a federal grand jury in Atlanta against four members of the Chinese People's Liberation Army (PLA), all allegedly members of PLA's 54th Research Institute, for hacking into the computer systems of credit reporting agency Equifax and stealing the personally identifiable information of approximately 145 million Americans, along with Equifax's trade secret database designs.

The defendants are alleged to have exploited a vulnerability in the framework software used by Equifax's online dispute portal. They used this to obtain login credentials that could later be used to further navigate Equifax's network. The defendants spent several weeks running queries to identify Equifax's database structure and searching for sensitive, personally identifiable information. Once they accessed files of interest, the defendants then stored the stolen information in temporary output files, compressed and divided the files, and ultimately were able to download and transfer out the data from Equifax's network. To evade detection, they routed traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location, used encrypted communication channels within Equifax's network to blend in with normal network activity, and deleted compressed files and wiped log

files on a daily basis. In total, the attackers obtained names, birth dates and social security numbers for nearly half of all American citizens.

In a related press conference, Attorney General Barr said that the theft of the credit information could be used to feed China' development of artificial intelligence tools and intelligence targeting packages.

In July last year, Equifax reached a $575 million settlement with the Federal Trade Commission, the Consumer Financial Protection, and 50 U.S. states and territories relating to the data breach, including establishment of a fund to compensate consumers affected by the breach. Equifax did not notice the intruders targeting of its databases for more than six weeks, despite members of its security team having notified that each of the company's vulnerable systems should be patched within 48 hours—a patch for the vulnerability was circulated, but because the company maintained an outdated list of computer systems administrators, the proper employees responsible for installing the patch never received it.

IV. Quinn Emanuel's Government Enforcement, China, IP and Trade Secrets Practices

Quinn Emanuel is an industry leader in dealing with Government Enforcement, IP and trade secrets litigation. Our Government Enforcement team is made up of more than 25 former federal and state prosecutors from around the U.S., as well as a robust team of Mandarin Chinese speaking attorneys – including a Chinese-speaking former federal prosecutor. We have a strong presence on the ground in the PRC and have deep experience counseling a wide variety of companies on PRC-related enforcement or litigation issues. We also protect and exploit the IP and trade secrets of companies that have developed some of the most valuable assets in this sphere across the globe. Our regular clients include Google, IBM, Qualcomm, SONY, Samsung, Symantec, and Johnson & Johnson. Legal publications rate our IP practice among the top IP in both the United States and Germany (where the vast majority of the EU's IP cases are filed).

- We have represented many of China's leading businesses, including its five largest state-owned banks, Alibaba (the leading e-commerce company) and Anta (the leading sportswear company) in U.S. litigation, much of it related to trade practices and PRC entities' obligations to disclose information to U.S. courts and regulators.
- We represent all manner of companies, including Chinese entities, in dealing with U.S. government enforcement risk, with particular focus on trade secret and other business crime investigations.
- We represented Waymo LLC, formerly Google's self-driving car program, in a lawsuit claiming misappropriation of trade secrets related to Waymo's self-driving LiDAR (Light Detection and Ranging) technology against Uber Technologies, Inc. and Ottomotto LLC. The parties reached a settlement on the fourth day of trial, after Waymo had presented much of its case-in-chief, granting Waymo a percentage of equity in Uber (valued at $245 million) as well as injunctive relief that assured Uber would not use Waymo's trade secret hardware and software self-driving car technology.
- We represented China-based Pangang Group Company in a criminal prosecution in the Northern District of California related to the alleged theft of trade secrets from DuPont. The United States government filed charges in 2012, alleging that Pangang conspired to steal titanium dioxide technology from DuPont. The case was considered one of the most significant prosecutions ever brought under the Economic Espionage Act, reaching front page coverage in the *Wall Street Journal*. In our defense of Pangang, we have staved off prosecution for over six years through a series of pretrial motions and by an appeal to the Ninth Circuit.
- We were lead counsel for Qualcomm in a patent infringement action Qualcomm brought against Apple in the International Trade Commission, alleging that Apple unlawfully imported and sold

iPhones that infringed five Qualcomm patents underpinning important features and functions in the iPhones. After a seven-day hearing, Administrative Law Judge McNamara issued an Initial Determination that recommended issuance of a limited exclusion order, which would have resulted in the exclusion of all iPhones and iPads without Qualcomm baseband processors from being imported into the United States. Apple settled with Qualcomm shortly thereafter.

* * * * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to:

Sam Williamson
Email: samwilliamson@quinnemanuel.com
Phone: +1 212 849 7455

Xiao Liu
Email: xiaoliu@quinnemanuel.com
Phone: +86 21 3401 8766

To view more memoranda, please visit www.quinnemanuel.com/the-firm/publications/

February 2020