# Research Integrity & Undue Foreign Influence

## Indictment of Chinese Hackers Serves as Further Warning to Companies and Research Organizations to Strengthen IT Security

### Companies need to strengthen and test data security across all dimensions – physical, digital, administrative, social

The Department of Justice unsealed on July 22, 2020 an indictment from earlier this month, which charges two Chinese nationals with hacking into the computer systems of hundreds of entities and individuals across the world and stealing terabytes of data, including intellectual property and trade secrets, and trying to steal even more data. Among the hackers' victims were biotech networks and firms developing vaccines, treatments, and testing technology for COVID-19.

## Hacking Efforts Have Been in Process for Years…

A federal grand jury in Spokane, Washington returned an 11-count indictment charging Xiaoyu Li and Jiazhi Dong, both currently in China, with conspiracy to commit computer fraud, conspiracy to commit trade secret theft, conspiracy to commit wire fraud, unauthorized access of a computer, and aggravated identity theft. Prosecutors say Li and Dong, who were trained in computer applications technologies at the same Chinese university, worked together for more than a decade targeting high-tech companies in more than 10 countries. Three of the U.S. companies targeted were in Massachusetts (a pharmaceutical company, medical device engineering company, and a software firm) and some of the other U.S. companies were pharmaceutical companies.

## … And Are Often Sponsored by Government Entities

According to the indictment, the two defendants in some instances worked with and were assisted by the Chinese Ministry of State Security (MSS). MSS Officers allegedly claimed to be researchers at the "Guangdong Province International Affairs Research Center" when in fact they were intelligence officers working for the Guangdong State Security Department. MSS encouraged the two defendants to steal material on military satellite programs, wireless networks and communication systems, high-powered microwave and laser systems, and a counter-chemical weapons system, according to the allegations. The indictment alleges that when they were stealing information of interest to the MSS, the defendants mostly obtained data through computer fraud against research institutions and corporations. In some instances, the indictment says, defendants provided an MSS Officer with email accounts and passwords belonging to clergymen, dissidents and pro-democracy activists who could then be targeted. The MSS Officer allegedly gave help to them as well, providing malicious software after one of the hackers struggled to compromise the mail server of a Burmese human rights group.

While the indictment does not accuse the two defendants of actually obtaining COVID-19 research, it does underscore the extent to which scientific innovation has been a top target for foreign governments and criminal hackers looking to know what U.S. companies are developing during the pandemic. The hackers in this case researched vulnerabilities in the computer networks of biotech firms and diagnostic companies that were developing vaccines and testing kits and researching antiviral drugs. The indictment renews the warning to life sciences businesses to keep an eye on their IT security from a physical, administrative, and social perspective.

# Research Integrity & Undue Foreign Influence

## For more information about these developments, please contact a member of our Foreign Influence and Compliance team:

**Christine G. Savage**
Practice Group Leader – Healthcare
617-248-4084 | csavage@choate.com

**Diana K. Lloyd**
Practice Group Leader – Government Enforcement & Compliance
617-248-5163 | dlloyd@choate.com

**Mark McPherson**
Associate
617-248-4992 | mmcpherson@choate.com

**Melissa Bayer Tearney**
Department Co-Chair – Litigation
617-248-4068 | mtearney@choate.com

**Danielle Pelot**
Partner
617-248-4007 | dpelot@choate.com