COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 3, Number 4. February 20, 2020
Indictment of Chinese hackers highlights need for effective data protection protocols

By Sascha Matuszak

Four Chinese nationals have been charged with orchestrating the hack into Equifax servers that compromised the sensitive data of more than half of all American citizens, as well as millions of citizens of the United Kingdom and Canada. According to a United States Department of Justice news release, the Chinese nationals Wu Zhiyong, Wang Qian, Xu Ke and Liu Lei are "members of the [People's Liberation Army] PLA's 54th Research Institute, a component of the Chinese military."[1]

"This was a deliberate and sweeping intrusion into the private information of the American people," said Attorney General William P. Barr, who made the announcement. "Today, we hold PLA hackers accountable for their criminal actions, and we remind the Chinese government that we have the capability to remove the Internet's cloak of anonymity and find the hackers that nation repeatedly deploys against us. Unfortunately, the Equifax hack fits a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."

The indictment[2] contains detailed information on the hack, including the exploit the hackers used, the actions taken within Equifax's database, the scope of the data stolen, and tactics used to prevent detection.