

[Banking and Finance Law Daily Wrap Up, CRIMES AND OFFENSES— Criminal indictment alleges Chinese military personnel hacked Equifax's computer systems, \(Feb. 10, 2020\)](#)

Banking and Finance Law Daily Wrap Up

[Click to open document in a browser](#)

By [Thomas G. Wolfe, J.D.](#)

The U.S. government has charged four members of the Chinese People's Liberation Army with computer fraud, economic espionage, and wire fraud for allegedly stealing millions of Americans' sensitive personal information and certain trade secrets of the credit reporting agency.

In keeping with a federal grand jury's criminal indictment filed with the federal district court in Atlanta, Ga., the United States government has [charged](#) four members of the "54th Research Institute" of the Chinese People's Liberation Army (PLA) with hacking into the computer systems of Equifax, Inc., one of the three nationwide consumer credit reporting agencies, and "stealing Americans' personal data and Equifax's valuable trade secrets." Alleging that these four individuals "conspired with each other" to unlawfully gain and maintain unauthorized access to Equifax's computers in 2017, the nine-count indictment brought by the U.S. Justice Department on behalf of the U.S. government alleges that the PLA defendants committed various acts of computer fraud, economic espionage, and wire fraud by stealing the "sensitive, personally identifiable information of approximately 145 million American victims," and by stealing Equifax's "data compilations and database designs" (*U.S. v. Zhiyong*, Case No. 2-20-CR046).

Stating in a Feb. 10, 2020, release that the criminal indictment addresses a "deliberate and sweeping intrusion into the private information of the American people," U.S. Attorney General William Barr, [asserted](#) that the United States government is holding the "PLA hackers accountable for their criminal actions," and reminding 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." He added, "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 Federal Bureau of Investigation worked with the Justice Department and U.S. Attorney's Office to facilitate obtaining the criminal indictment. FBI Deputy Director David Bowdich remarked that "[t]his is not the end of our investigation; to all who seek to disrupt the safety, security and confidence of the global citizenry in this digitally connected world, this is a day of reckoning."

Backdrop. In September 2017, Equifax announced that more than 143 million Americans potentially had their personal information compromised in a massive cybersecurity incident at the company. According to Equifax at the time, the computer hackers exploited a website application vulnerability to gain access to certain consumer files from mid-May through July 2017. The company communicated various preliminary estimates about the personal identifying information of consumers that was accessed by the hackers—including names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and certain dispute documents (see [Banking and Finance Law Daily](#), Sept. 8, 2017).

According to the Justice Department, the PLA defendants took steps "to evade detection throughout the intrusion" by routing computer traffic "through approximately 34 servers located in nearly 20 countries to obfuscate their true location." In addition, the defendants allegedly "encrypted the communication channels within Equifax's network to blend in with normal network activity," and then "deleted compressed files and wiped log files on a daily basis in an effort to eliminate records of their activity."

Criminal indictment. The U.S. criminal indictment sets forth nine counts against the PLA members (Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei), including: computer fraud conspiracy; computer fraud and abuse—intentional damage; computer fraud and abuse—unauthorized access; conspiracy to commit economic espionage; economic espionage; conspiracy to commit wire fraud; and three counts concerning wire fraud. Further, the indictment calls for the PLA defendants to forfeit to the U.S. government, upon their conviction, any interests in property obtained or derived from proceeds as a result of their federal law violations.

Besides the charges pertaining to U.S. citizens, the indictment also states that the PLA hackers "obtained personally identifiable information belonging to nearly a million citizens of the United Kingdom and Canada."

Attorneys: Byung J. Pak, Samir Kaushal, and Thomas J. Krepp of the U.S. Attorney's Office in Georgia, and Benjamin Fitzpatrick and Scott McCulloch of the U.S. Justice Department in Washington, D.C., for the United States.

Companies: Equifax Inc.

LitigationEnforcement: CrimesOffenses CyberPrivacyFeed EnforcementActions FairCreditReporting
GeorgiaNews IdentityTheft Privacy UDAAP Enforcement