Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Red Army Equifax Hackers Indicted

March 4, 2020

A federal grand jury has indicted four members of the Chinese People's Liberation Army (PLA) for hacking into the Equifax computer system and stealing the personal identifying information of "nearly 150 million Americans." The indictments charge offenses under federal wire fraud, computer intrusion, economic espionage, and conspiracy laws. Attorney General Barr's statement announcing the indictment noted that 80% of federal economic espionage prosecutions have implicated the Chinese government. The indictment presents a partial view of the criminal law consequences that may attend a mass data breach, but the indictment is likely designed for purposes other than eventual prosecution.

Background

Equifax conducts credit checks on behalf of financial institutions and other business entities. The indictment and an earlier House committee majority staff report allege that the four defendants accessed an Equifax server in Georgia through a system backdoor. Once in, they spent several weeks sweeping the system for the names, addresses, birth dates, social security numbers, and driver's license numbers of millions of individuals. Equifax eventually discovered the breach, patched the hole, and notified authorities and the public. Equifax has agreed to pay more than $5.75 million to settle claims relating to the data breach.

Statutes

The indictment charges violations of four of the criminal laws designed to protect against computer intrusions (alternatively known as hacking or unauthorized access) and other forms of data breach: the Computer Fraud and Abuse Act (CFAA); the Economic Espionage Act; the Wire Fraud Act; and the conspiracy statute. (For a discussion of these and other statutes that protect against such intrusions (CRS Report R45631).

The CFAA outlaws seven computer hacking offenses, ranging from simple trespassing to espionage (CRS Report 97-1025). One offense covers intrusions that involve stealing information from a protected computer system. "Protected computer" means any computer connected to the Internet ("computer … which is used in or affecting interstate or foreign commerce or communication"). The offense is a five-year felony if the information is worth $5,000 or more or if the intrusion is committed with an eye to another state or federal crime. The Chinese army defendants allegedly acted as accomplices for colleagues who hacked into an Equifax computer and bundled up masses of personal information worth more than $5,000 to support an economic espionage operation. Accomplices (aiders and abettors) share liability equally with those who actually commit the crime. (CRS Report R43769). The indictment also

calls for the confiscation upon conviction of any equipment or other property used to commit the violation of the Computer Fraud and Abuse Act.

A CFAA second offense covers damaging a computer system during unauthorized access. "Damage" includes "any impairment to the integrity … of data … or [a computer] system". The accompanying sanctions correspond to those for the theft of information under the statute. The indictment charges the defendants with acting as accomplices in the damage resulting from the intrusion into the Equifax system and the massive harvesting of its data.

Under the Economic Espionage Act, economic espionage occurs when an individual surreptitiously downloads someone else's trade secrets for the benefit of a foreign government or entity. (CRS Report R42681). Offenders face the prospect of up to 15 years in prison, a fine of up to $5 million, and the confiscation of any equipment or other property used to commit the crime. The Red Army defendants stand accused of downloading Equifax's trade secret data for the benefit of the Chinese government.

It is hard to engage in computer intrusion or economic espionage without also coming within reach of the wire fraud statute. Wire fraud consists of the use of the telephone, email, the Internet, or some other form of wire communications as part of a scheme to cheat someone out of their tangible or intangible property. (CRS Report R41930). The penalties are severe – up to 20 years in prison and a fine of up to twice the profit or loss associated with the crime or $250,000, whichever is more. The indictment alleges that the defendants acted as accomplices for confederates who used deception to gain wire access to the Equifax computer system. In doing so, they purportedly deprived the company of exclusive control of personal identifying information relating to individuals who in total make up almost half of the population of the United States.

The indictment lists as separate offenses the defendants' conspiracies to violate the CFAA, the Economic Espionage Act, and the Wire Fraud Act. Conspiracy is the agreement of two or more to commit a crime. (CRS Report R41223). Conspiracies to violate the Economic Espionage Act or the Wire Act come with the same penalties as the underlying offenses (imprisonment for up to 15 years and 20 years, respectively). Conspiracy to violate the CFAA falls under the general conspiracy statute which carries a prison term of up to five years.

Chances of a Trial

The Justice Department likely sought the indictments for reasons other than prosecution. In fact, prosecution of the Red Army defendants seems improbable. Federal prosecution of defendants located outside the U.S. ordinarily depends on extradition under a treaty. (CRS Report 98-958). The U.S. does not have an extradition treaty with China. The indictment, however, might limit the defendants' future travel. Once found in the country with whom the U.S. has an extradition treaty, the defendants would face possible extradition. The U.S. has extradition treaties with most countries in this hemisphere, with most European nations, and with many African and Southeast Asian countries.

Even with a treaty, however, extradition can be problematic in computer hacking cases. Extradition treaties describe extraditable offenses in one of two ways. The older agreements identify a list of specific extraditable offenses. The newer treaties make extraditable any crime punishable under the laws of both the prosecuting country and the country where the accused is located. The crimes detailed in the indictment may not fit neatly in either category. Moreover, in the context of a particular treaty, economic espionage may fall within the pure political offense exception that renders treason, sedition, and espionage non-extraditable offenses. All of which may explain why the Red Army members indicted on similar charges in 2014 remain at large.

Congressional Activity

Much of the recent legislative activity related to the Equifax intrusion has focused on non-criminal matters. A few proposals, however, have suggested adjustments to the Computer Fraud and Abuse Act or the Economic Espionage Act. For example, the proposed Active Cyber Defense Certainty Act, H.R. 3270 (Representative Graves) would amend the CFAA to exempt from CFAA's prohibitions certain acknowledged computer defense activities. Similarly, the DEFEND Act, S. 1865 (Senator Harris), would enlarge the overseas reach of the Economic Espionage Act (EEA) and further encourage private enforcement of the EEA.

Author Information

Charles Doyle
Senior Specialist in American Public Law

Disclaimer