December 20, 2022

Theft of Federal Funds Highlights Expanding Cyber Threat from Foreign Actors

The Secret Service has reported that APT41, a hacking organization, stole roughly $20 million in federal COVID-19 relief funds by obtaining access to the computer systems of a number of U.S. states beginning in mid-2020.[1] According to the Secret Service, APT41 is a "Chinese state-sponsored, cyberthreat group that is highly adept at conducting espionage missions and financial crimes for personal gain."[2] While experts are uncertain regarding whether the breach by APT41 was ordered by the PRC government or merely tolerated, the Secret Service announcement marks the first public confirmation by a federal agency of a state-affiliated hacking group breaching U.S. cyber defenses to steal federal funds. According to the government, the hackers obtained unemployment insurance funds and Small Business Administration loans from more than a dozen states.[3] The true scope of the breach remains unclear, with officials speculating that government networks in all 50 states were likely targeted.[4] The Secret Service has further linked the APT41 intrusion to the organization's broader efforts to access and interrogate state networks.[5]

APT41's cyber operation is only the latest in a series of financial crimes and acts of espionage perpetrated by state-linked organizations against both private and public entities in the United States. However, the group's decision to target federal funds represents a novel and potentially provocative escalation in the group's criminal activities, one that appears to have been made possible by the operational experience the group gained in accessing and gathering personal data of American citizens. The theft of U.S. government funds by APT41 is illustrative of the landscape of expanding cyber threats the American national security apparatus must navigate.

Key Takeaways

- Cyber fraud by state-sponsored actors against individual American citizens could have legal implications for corporate custodians of personal data. While it remains unclear whether the APT41 attack was sanctioned by the PRC government, the breach of government networks by a state-sponsored hack would shake the widely held assumption that such foreign actors only prosecute cyberattacks for the purposes of espionage. The new possibility of foreign-government-sponsored

1 The U.S. Secret Service did not issue its own report about this incident but is reported to have confirmed public news reports about the event. Sarah Fitzpatrick & Kit Ramgopal, *Hackers Linked to Chinese Government Stole Millions in Covid Benefits, Secret Services Says*, NBC NEWS (Dec. 5, 2022), available here.

2 *Id.*

3 Sean Lyngaas, *US Secret Service Accuses Chinese Government-Linked Hackers of Stealing $20 Million in Covid Relief*, CNN (Dec. 5, 2022), available here.

4 Fitzpatrick & Ramgopal, *supra* note 1.

5 *Id.*

breaches causing harm to individual consumers potentially alters the responsibilities of corporate data custodians. For instance, the credible threat of harm faced by consumers after such an attack could lead courts to find sufficiently concrete harm for class certification in a suit against a company targeted by such an attack, where before an attack that only resulted in access to data likely would not result in a such a finding.[6] The increased likelihood of harm to individuals could also affect companies' reporting obligations following a breach by a state-sponsored entity, as many cybersecurity regulations exempt breach targets from notification procedures where no harm is likely to arise from the cyber incident.[7]

- Criminal indictments are only one aspect of efforts to deter foreign hacking groups. The DOJ's efforts to deter state-sponsored cybercrimes through criminal indictments against state-affiliated hackers have not produced the desired effect of mitigating cybercrime by actors with affiliations to foreign states.[8] The limited ability of domestic law enforcement to prevent cyber threats has already lead to an increased emphasis on other strategies, including greater reliance on offensive cyber measures, investment in defensive cyber capabilities and diplomatic efforts as part of the "all tools" approach described by Deputy Attorney General Lisa Monaco in her July 2022 keynote address at the International Conference on Cyber Security.[9]

We will continue to provide updates on developments in cyber threats.

* * *

6 *See, e.g.*, *TransUnion* v. *Ramirez*, 142 S. Ct. 2190 (2021).

7 *See, e.g.*, Arkansas Personal Information Protection Act, available here; Connecticut General Statutes 36a-701b, available here; Delaware Code, Title 6, Chapter 12B, available here.

8 *See, e.g.*, *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research*, Department of Justice (July 19, 2021), available here.

9 *Deputy Attorney General Lisa O. Monaco Delivers Keynote Address at International Conference on Cyber Security (ICCS 2022)*, Department of Justice (July 19, 2022), available here.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Neil Chitrao, Katherine Fang and Cole Rabinowitz contributed to this Client Memorandum.