CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

September 29, 2021

The Honorable Christopher A. Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Wray:

Earlier this summer, a Florida-based software company was the victim of a ransomware attack that compromised between 800 and 1,500 businesses around the world.[1] Although the Federal Bureau of Investigation (FBI) reportedly obtained a digital decryptor key that could have unlocked affected systems, it withheld this tool for nearly three weeks as it worked to disrupt the attack, potentially costing the ransomware victims—including schools and hospitals—millions of dollars.[2] We request information to understand the rationale behind the FBI's decision to withhold this digital decryptor key and the agency's approach to responding to ransomware attacks.

As you are aware, cyber attacks, including ransomware attacks, have become more frequent and severe in nature. Estimates indicate "304 million ransomware attacks worldwide in 2020,"[3] costing over $19 billion in total economic damage in the United States in 2020.[4] Statistics from the same year show the "average ransom payment is $154,108."[5] In fact, the

---

[1] *Up to 1,500 Businesses Could Be Affected by a Cyberattack Carried Out by a Russian Group*, New York Times (July 26, 2021) (online at www.nytimes.com/2021/07/06/technology/kaseya-cyberattack-ransomware-revil.html).

[2] *Id.*; Ellen Nakashima and Rachel Lerman, *FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers*, Washington Post (Sept. 21, 2021) (online at www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html).

[3] *Annual Number of Ransomware Attacks Worldwide from 2016 to 2020*, Statista (July 22, 2021) (online at www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/#:~:text=According%20to%20an%20annual%20report%20on%20global%20cyber,%28in%20millions%29%20Number%20of%20ransomware%20attacks%20in%20millions).

[4] Emsisoft Blog, *The Cost of Ransomware in 2021: A Country-by-Country Analysis* (Apr. 27, 2021) (online at https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/).

[5] *Id.* This average does not include a particular ransomware strain called STOP whose average demand is $490.

largest known ransomware attack on U.S. infrastructure to date perpetrated against Colonial Pipeline "resulted in a six-day shutdown" and a $4.4 million ransom and "caused widespread disruption to the fuel supply chain, resulting in gas prices hitting a six-year high."[6] The growing threat of ransomware attacks requires our federal government agencies—especially the FBI—to respond quickly and effectively to prevent or minimize the damage from these attacks.

Public reporting raises questions about the FBI's response to this summer's ransomware attack. The FBI has stated that it withheld the ransomware key it had previously acquired so the Bureau could engage in an operation to disrupt the Russian-based hackers without tipping them off.[7] Before the FBI could execute its plan, however, the hackers reportedly disappeared and their platform went offline.[8] During this delay, many businesses, schools, and hospitals suffered lost time and money, especially in the midst of the COVID-19 public health crisis.

We request a briefing from the FBI on its legal and policy rationale for withholding the digital decryptor key as it attempted to disrupt this cyber attack, and the FBI's overall strategy for addressing, investigating, preventing, and defeating ransomware attacks. Ransomware hackers have shown their willingness and ability to inflict damage on various sectors of the U.S. economy. Congress must be fully informed whether the FBI's strategy and actions are adequately and appropriately addressing this damaging trend.

To schedule the briefing, please contact Committee majority staff at (202) 225-5051 or minority staff at (202) 225-5074 no later than October 6, 2021. The Committee on Oversight and Reform is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. Thank you for your cooperation with this request.

Sincerely,

Carolyn B. Maloney
Chairwoman

James Comer
Ranking Member

[6] Emsisoft Blog, *Ransomware Statistics for 2021: Q2 Report* (July 6, 2021) (online at https://blog.emsisoft.com/en/38864/ransomware-statistics-for-2021-q2-report/).

[7] Ellen Nakashima and Rachel Lerman, *FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers*, Washington Post (Sept. 21, 2021) (online at www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html).

[8] *Id.*