

ONE HUNDRED SEVENTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

August 30, 2021

Mr. Charles Carmakal
Senior Vice President and Chief Technology Officer
FireEye-Mandiant
601 McCarthy Boulevard
Milipitas, CA 95035

Dear Mr. Carmakal:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Wednesday, July 20, 2021, at the hearing entitled “Stopping Digital Thieves: The Growing Threat of Ransomware.” I appreciate the time and effort you gave as a witness before the Committee on Energy and Commerce.

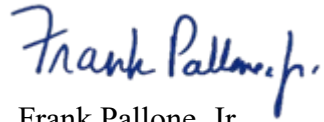
Pursuant to Rule 3 of the Committee on Energy and Commerce, members are permitted to submit additional questions to the witnesses for their responses, which will be included in the hearing record. Attached are questions directed to you from certain members of the Committee. In preparing your answers to these questions, please address your response to the member who has submitted the questions in the space provided.

To facilitate the printing of the hearing record, please submit your responses to these questions no later than the close of business on Monday, September 13, 2021. As previously noted, this transmittal letter and your responses will all be included in the hearing record. Your written responses should be transmitted by e-mail in the Word document provided to Austin Flack, Policy Analyst, at austin.flack@mail.house.gov. To help in maintaining the proper format for hearing records, please use the document provided to complete your responses.

Mr. Charles Carmakal
Page 2

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Austin Flack with the Committee staff at (202) 225-2927.

Sincerely,

A handwritten signature in blue ink that reads "Frank Pallone, Jr." in a cursive style.

Frank Pallone, Jr.
Chairman

Attachment

Mr. Charles Carmakal

Page 3

cc: The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy and Commerce

The Honorable Diana DeGette
Chair
Subcommittee on Oversight and Investigations

The Honorable H. Morgan Griffith
Ranking Member
Subcommittee on Oversight and Investigations

Attachment—Additional Questions for the Record

**Subcommittee on Oversight and Investigations
Hearing on
“Stopping Digital Thieves: The Growing Threat of Ransomware”
July 20, 2021**

Mr. Charles Carmakal, Senior Vice President and Chief Technology Officer, FireEye-Mandiant

The Honorable Frank Pallone, Jr. (D-NJ)

1. The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.
 - a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?
 - b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

The Honorable Diana DeGette (D-CO)

1. I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry’s response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

The Honorable H. Morgan Griffith (R-VA)

1. Employees warned Kaseya’s higher-ups for years about critical security flaws in its software but their concerns were brushed off, former workers told Bloomberg.¹ Several staffers quit in frustration or were fired after repeatedly sounding the alarm about failings in the IT firm’s cybersecurity practices. Between 2017 and 2020, employees reported “wide-ranging cybersecurity concerns” to their superiors, claiming that Kaseya used outdated code, implemented poor encryption, and didn’t routinely patch its software and servers, Bloomberg reports.² Now, Kaseya is at the center of a massive ransomware attack that’s ensnared more than 1,000 companies worldwide.³
 - a. Do organizations place more trust in notifications of system vulnerabilities from outside groups, like FireEye-Mandiant, over their own internal cybersecurity departments?
 - b. If organizations are more inclined to listen to warnings from outside groups, should we continue to outsource cybersecurity monitoring to ensure more companies incorporate their suggestions?
 - c. How do we encourage organizations from local governments to private companies to seriously consider the severity of cyber threats at the point when they are discovered on their systems, instead of at the time of a ransomware attack?
2. In October 2020, the U.S. Department of Treasury’s Office of Foreign Assets (OFAC) issued an advisory guidance to companies providing services to victims of ransomware attack payments.⁴ The advisory warns against payments from U.S. persons with individuals or entities Specially Designated Nationals and Blocked Persons List (SDN List), and other blocked persons and those covered by comprehensive country or region embargoes. The advisory states that a violation by a non-U.S. person, which causes a U.S. person to violate any sanctions, or U.S. persons facilitating actions of a non-U.S. persons in an effort to avoid sanctions regulations, are also prohibited. The advisory states that OFAC may impose civil penalties based on strict liability. In summary, there are potential sanction risks associated with

¹ *Kaseya Failed to Address Security Before Hack, Ex-Employees Say*, Bloomberg (July 10, 2021).

² *Kaseya's Staff Sounded the Alarm About Security Flaws for Years Before Ransomware Attack*, Gizmodo (July 11, 2021).

³ *REvil Gang Takes Credit for Massive Kaseya Attack and Asks for \$70 Million Ransom*, Gizmodo (July 5, 2021).

⁴ U.S. Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020) (home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf).

facilitating a ransomware payment. Do you think this OFAC guidance is helpful or hurtful to companies providing services to victims of ransomware attacks?

3. During the hearing, you mentioned that smaller organizations do not have the IT resources to have the necessary level of cyber hygiene to prevent ransomware attacks. Are there ways to incentivize companies to invest in their information technology systems so that they are more resilient against ransomware attacks?
4. During the hearing, you also mentioned smaller organizations do not know about digital forensics. You mentioned the need for government involvement in the indictments of individuals involved in these attacks, especially for attacks on small businesses.
 - a. If these smaller organizations do not have the staff and resources to revamp their cyber security hygiene, can you elaborate on the most beneficial support the federal government can provide to small businesses to deter further ransomware attacks?

The Honorable Michael C. Burgess, M.D. (R-TX)

1. Many cybersecurity experts do not believe a federal reporting requirement for ransomware and other cyber-attacks is helpful because the victims often do not have a full understanding of the attack until 24 hours or more later, and the federal government can inhibit an effective response by getting involved too early in recovery efforts.
 - a. Do you believe there should be a federal reporting requirement for cyber-attacks, particularly ransomware attacks? Why or why not?

The Honorable Gary Palmer (R-AL)

1. I am told that FireEye has a wealth of information about cybercrime actors. One of my constituents tells me that they have a list of 3,300 companies that have had their private data – information about them, their corporate secrets, and their clients and customers – put on a ransomware leak site and been told that if they didn't pay a ransom, even more documents would be leaked. Mr. Reiner's group shared in their report that 199 cryptocurrency addresses received 80% of all the payments that were made for ransomware, and that just 25 addresses accounted for 46% of all ransom payments.
 - a. With the skills FireEye and Mandiant have in attribution, would you say that you could tell us who those people are? Do you know the names of the people behind these attacks? And if you do, what would you recommend we do to disrupt them?