GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH 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

September 20, 2017

The Honorable Thomas E. Price, M.D.
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Secretary Price:

According to both news reports and recent public statements, pharmaceutical company Merck's ability to supply some of its products may be affected due to lingering effects of the malware strain commonly known as "NotPetya."[1,2] While it has long been understood that Merck was among those infected by this malware, the revelation that it continues to affect Merck's operations adds to the growing list of concerns about the potential consequences of cyber threats to the health care sector. It is important, therefore, for the Committee to understand the details of this event and the response of the Department of Health and Human Services (HHS) so that we can work together to ensure appropriate lessons are identified and addressed. Learning from this event will not only benefit the health care sector, but also the millions of patients who depend on the availability of its products and services.

On June 27, 2017, a malware infection spread across the globe, affecting the networks and digital assets of companies across a wide range of sectors. The malware – commonly referenced as "Petya," "NotPetya," "NietPetya," among other names – leveraged a known vulnerability to gain access to systems and networks which were then encrypted, rendering them useless to the owners of those assets.[3] While the malware was largely contained after the initial

---

[1] Hamza Shaban & Ellen Nakashima, *Pharmaceutical giant rocked by ransomware attack,* THE WASH. POST, June 27, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/.

[2] *Merck Announces Second-Quarter 2017 Financial Results*, MERCK & CO, INC, July 28, 2017, http://investors.merck.com/news/press-release-details/2017/Merck-Announces-Second-Quarter-2017-Financial-Results/default.aspx.

[3] While this exploit was originally believed to be "ransomware," some have suggested it is more appropriately considered a "wiper" due to the inability of the authors – or attackers – to decrypt affected systems, even if the ransom was paid by a victim.

outbreak, it successfully compromised businesses around the world. Known victims came from a variety of sectors including, but not limited to, shipping, food, marketing, oil, and legal. It was widely reported at the time that Merck was among those affected by the NotPetya malware strain.[4]

Until recently, there was little information about the magnitude of the effect on Merck's operations. In its second-quarter 2017 financial outlook, however, Merck provided more detail. It stated:

> On June 27, 2017, the company experienced a network cyber-attack that led to disruption of its worldwide operations, including manufacturing, research and sales operations. While the company does not yet know the magnitude of the impact of the disruption, which remains ongoing in certain operations, it continues to work to minimize the effects.
>
> The company is in the process of restoring its manufacturing operations. To date, Merck has largely restored its packaging operations and has partially restored its formulation operations. The company is in the process of restoring its Active Pharmaceutical Ingredient operations but is not yet producing bulk product. The company's external manufacturing was not impacted. Throughout this time, Merck has continued to fulfill orders and ship product. [5]

While there is no evidence, to date, that Merck's manufacturing disruption has created a risk to patients, it certainly raises concerns. For example, in a recent update on national vaccine supply, the CDC reported that Merck would not be distributing certain formulations of the Hepatitis B vaccine.[6] While it is unclear whether this is related to the NotPetya disruption, and much of the supply can be filled by other manufacturers, it does raise questions about how the nation is prepared to address a significant disruption to critical medical supplies.

Though cybersecurity has been of increasing concern over the last several years, especially within the healthcare sector, the NotPetya infection represents a new challenge in that it is one of the first known instances in which a malware infection disrupted a company's physical manufacturing capabilities.[7] While Merck was not the only company to suffer degraded capabilities due to the June 27 outbreak, Merck's role as a supplier of life-saving drugs and other medical products sets its infection and subsequent manufacturing issues apart and raises the possibility of more serious consequences for the health care sector as a whole.

With this in mind, the Committee requests a briefing by October 4, 2017 to better understand (1) what actions HHS has taken to understand and respond to the situation, and (2)

---

[4] *See supra* note 1.
[5] *See supra* note 2.
[6] https://www.cdc.gov/vaccines/hcp/clinical-resources/shortages.html#note1
[7] Michael Erman & Jim Finkle, *Merck says cyber attack halted production, will hurt profits*, REUTERS, July 28, 2017, https://www.reuters.com/article/us-merck-co-results-idUSKBN1AD1AO.

HHS's policies, plans, and procedures for addressing potential drug shortages or other associated consequences caused by cyber infections such as the NotPetya malware strain.

We appreciate your assistance with this request. If you should have any questions, please contact John Ohly or Jessica Wilkerson of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman
Committee on Energy and Commerce

Tim Murphy
Chairman
Subcommittee on Oversight
and Investigations

cc: The Honorable Frank Pallone, Jr., Ranking Member
Committee on Energy and Commerce

The Honorable Diana DeGette, Ranking Member
Subcommittee on Oversight and Investigations