United States Senate
WASHINGTON, DC 20510

April 1, 2024

Andrew Witty
Chief Executive Officer
UnitedHealth Group
UnitedHealth Group Center
990 Bren Road East
Minnetonka, Minnesota 55343

Dear Mr. Witty,

We write demanding information regarding the disastrous disruption of UnitedHealth Group's ("UHG") subsidiary Change Healthcare ("Change") by the ransomware group BlackCat, and seek answers about how its critical health care systems were breached, why the firm has suffered such an egregious and unexplained outage, and whether patient and provider data was compromised in the attack. Further, and importantly, we demand that UHG proactively advance payments for all claims – not just UHG claims – to providers so they can keep their doors open as you resolve this inexcusably lengthy shutdown of your systems.

While we recognize that UHG was indeed the victim of an outside attack, the entire sector is now the victim of UHG's lack of preparedness and built in redundancies, which could have potentially mitigated the widespread impact of the breach. The lessons from this cyber-attack and UHG's response to it have significant implications for the readiness and resiliency of the entire healthcare and public health sector – which is why UHG's transparency is of the utmost importance.

On February 21st, Change suffered a catastrophic cyberattack that took down its entire infrastructure, and left the American health care system "paralyzed."[1] Change had become "critical infrastructure" to the American health care system,[2] processing 15 billion health care transactions and $1.5 trillion in healthcare claims annually.[3] Because of the company's

[1] Reed Abelson and Julie Creswell, "Cyberattack Paralyzes the Largest U.S. Health Care Payment System," *New York Times* (New York, NY), March 5, 2024, https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.
[2] Stanton, *supra* note 3.
[3] "How to Deliver High Performance Healthcare Marketing," Change Healthcare, accessed March 15, 2024, https://www.changehealthcare.com/insights/deliver-high-performance-healthcare-marketing.

overwhelming reach—handling as many as one of every three patient records in the country—the breach of Change was tantamount to targeting the health care system in its entirety.[4]

The result of UHG's failure to properly safeguard against cyber threats and the subsequent, extended outage of its services has been dire. Providers were unable to fill prescriptions, verify patients' eligibility for treatment, and submit insurance claims.[5] Over three weeks later, the outage is not completely resolved. Patients, whose illnesses cannot be put on hold for UHG's failures, face uncertainty in accessing treatment and the prospect that their Personal Identifiable Information (PII) or Protected Health Information (PHI)—extremely private information—is now in the hands of criminals.

The disruption has also led to alarming downstream risks for the financial stability of the health care sector, especially for rural and small providers. With its systems still offline, the company is paying out far fewer insurance claims than usual.[6] Even as providers and practices verge on bankruptcy, UHG has not meaningfully cleaned up the damage. When providers have turned to the emergency lending program held out by UnitedHealth, they have received pitiful offers as low as $10.[7] Even when providers receive loans, the terms and conditions have been described as "shockingly onerous." UHG has allegedly modified its financial assistance program to provide more generous advance payments, announcing that $2 billion in fund have been advanced only after your initial loan program was harshly criticized, but providers are still struggling financially: in Connecticut, as of this writing, our providers report that they have yet to receive meaningful assistance from your company. Without a useable bridge program for providers, UHG's delayed efforts can be seen as little more than a public relations strategy to placate stockholders and win over public opinion.

The origin of this crisis can be traced back to 2021, when UHG moved to buy Change Healthcare.[8] At the time, UHG's subsidiary Optum was one of Change's primary competitors in the health care IT space.[9] Medical trade groups warned that the merger would not only result in a near-monopoly in health IT, but also give UnitedHealth Care—the country's largest insurer and a subsidiary of UHG—access to competitors' claims and policy information.[10] The Department of Justice (DOJ) sued unsuccessfully to block the deal, and the merger was allowed to proceed.[11]

---

[4] *Id.*
[5] Abelson and Creswell, *supra* note 1.
[6] Stanton, *supra* note 3.
[7] Maureen Tkacik, "UnitedHealth Exploits an 'Emergency' It Created," *The American Prospect*, March 10, 2024, https://prospect.org/health/2024-03-10-unitedhealth-exploits-emergency-change-ransomware-oregon/.
[8] Chris Stanton, "Corporate Greed Made the Change Healthcare Cyberattack Worse," *New York*, March 7, 2024, https://nymag.com/intelligencer/article/corporate-greed-made-the-change-healthcare-cyberattack-worse.html.
[9] *Id.*
[10] *Id.*
[11] U.S. Department of Justice, "Justice Department Sues to Block UnitedHealth Group's Acquisition of Change Healthcare," press release, February 24, 2022, https://www.justice.gov/opa/pr/justice-department-sues-block-unitedhealth-group-s-acquisition-change-healthcare.

UnitedHealth and Change became too big to fail, and then they did—disastrously. Accountability needs to fall on the companies responsible for the chaos. We ask for your responses to the following questions by April 15, 2024:

1. How did the hackers behind the Change cyberattack initially breach the company and gain such significant access to its systems?

2. Please provide a detailed timeline of all events related to the breach, including the date and background on the discovery, response, and remediation of compromised systems or disabled services.

3. According a claim from an affiliate of the BlackCat group, up to four terabytes of data were stolen in the hack, including Medicare and insurance data.[12] What data, including provider or patient data, was compromised in the attack?

    a. What, if any, processes have Change Healthcare and UnitedHealth Group used to identify compromised provider or patient data?

    b. Have Change Healthcare and UnitedHealth Group notified impacted providers or patients regarding their compromised data?

4. Why has it taken so much time for the Change Healthcare and UnitedHealth Group systems to recover from the attack, and why did Change not have sufficient redundancy to prevent an outage? Please describe Change's plans to respond to potential cyberattacks and why those plans appear to have failed.

5. What, if any, cybersecurity improvements have Change Healthcare and UnitedHealth Group made since the attack?

    a. What assurances do providers and patients have that Change's infrastructure is secure against further breaches or disruptions?

6. Reporting indicates the BlackCat was paid $22 million in bitcoin in early March, and that the ransomware group may have stolen those funds from the affiliated hacker in possession of Change's data.

    a. Did Change Healthcare or UnitedHealth Group, or anyone acting on their behalf, make a ransomware payment, and if so for what purposes?

    b. What steps have BlackCat or its affiliates taken in response to the payment of a ransom, and does Change have any reliable assurances that provider or patient data has been deleted or will not be shared?

[12] https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/

7. Regarding UnitedHealth Group's financial assistance program:

    a. Has UnitedHealth Group proactively contacted any health care providers regarding cash assistance? If so, how have you contacted them? If not, why not?

    b. Please describe the application process to request funds.

    c. Please describe any terms and conditions providers are required to agree to in order to access advance payments.

8. On March 7, 2024, you announced a switch from a loan program, which was heavily criticized by providers, to an advance payment program.

    a. Why didn't UHG immediately begin create an advance payment program once it was clear an extended shutdown of Change was likely?

    b. Why did you instead opt for a loan program with "onerous" conditions?

9. On March 18, 2024, you announced your company "has advanced more than $2 billion thus far through multiple initiatives."[13]

    a. What percentage of providers serviced by Change have received an advance payment from UnitedHealth Group?

    b. What has been the average payment?

    c. On average, what percentage of the revenue gap providers are experiencing has UHG filled? Please provide percentages for UHG-only claims and claims for all payers.

10. UnitedHealth Group's financial assistance program is intended to cover UnitedHealthcare claims, but obviously, UnitedHealthcare claims only make up a fraction of providers' revenue. UnitedHealth Group has announced a program "of last resort" for providers "who work with a payer who has opted not to advance funds to providers." Whether or not UHG advances payments for other payers' claims will be determined on a "case-by-case basis."[14]

    a. Considering this problem stems directly and solely from Change's nearly month-long shutdown, why is UnitedHealth Group relying on other payers to fill the cash flow gap?

---

[13] https://www.unitedhealthgroup.com/newsroom/2024/2024-03-18-uhg-cyberattack-status-update.html
[14] https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html

b. How many providers have requested UnitedHealth Group advance payments on behalf of other payers, and how many of those requests have been honored?

11. Has UnitedHealth taken steps or discussed acquiring any practice or provider impacted by the Change attack? If so, please name what entities and provide information about this attempted acquisition.

12. Reporting indicates that UnitedHealth subsidiary Optum has attempted to accelerate its purchase of at least one medical practice that faced bankruptcy if it did not receive an immediate cash infusion, while avoiding patient protections and other conditions on the purchase sought by the state health authority, under the guise of the emergency it created.[15] UnitedHealth's attempts to "profit[] from the desperation" created by its own failures are unconscionable.[16]

    a. Has UnitedHealth agreed to the conditions sought by the Oregon Health Authority in connection with its purchase of The Corvallis Clinic?

    b. Has Optum made new offers to purchase any practices since the February 21st attack? If so, how many?

        i. How many of the target practices faced financial consequences resulting from the February 21st attack?

        ii. How many of these practices were in negotiations with Optum prior to the attack?

    c. Have other UnitedHealth subsidiaries attempted to "profit[] from the desperation" by making advantageous deals or other business arrangements with companies facing financial hardship as a result of the February 21st attack?

Thank you for your attention to this important matter.

Sincerely,

Richard Blumenthal
Chair
Subcommittee on Privacy, Technology, and the Law
United States Senate

Josh Hawley
Ranking Member
Subcommittee on Privacy, Technology, and the Law
United States Senate

[15] Tkacik, *supra* note 8.
[16] *Id.*