

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 30, 2024

The Honorable Lina S. Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chair Khan and Chair Gensler:

I write to request that your agencies investigate UnitedHealth Group's (UHG) negligent cybersecurity practices, which caused substantial harm to consumers, investors, the health care industry, and U.S. national security. The company, its senior executives, and board of directors must be held accountable.

On February 21, 2024, UHG announced that the computer systems of its subsidiary Change Healthcare had been infected with ransomware. Change Healthcare serves as a health care clearinghouse transmitting medical and dental claims and remittances, prior authorization, and patient eligibility and benefits verification. UHG opted to take down and rebuild its systems from scratch, which resulted in an across-the-board outage of the company's services. The company was able to restore some of these services in weeks, but others stayed offline for more than two months. Patients have been directly harmed. Patients were reportedly unable to collect prescriptions from pharmacies and lost access to care as some providers have closed or reduced hours to manage the outage. This incident also had a disastrous impact on other companies in the health care industry. Providers have reported going without pay, taking out loans, using personal funds, and even closing.

The harms are not limited to those caused by the outage. UHG has publicly stated that sensitive health data about a substantial portion of the population may have also been stolen. If these health records are made public — as hackers have done in other incidents — it could cause enormous harm to the victims. Moreover, UHG has confirmed that the stolen data likely includes information on military personnel and other U.S. government employees. Those records could be exploited by adversary countries, like China and Russia, to cause serious harm to U.S. national

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

security.

This incident and the harm that it caused was, like so many other security breaches, completely preventable and the direct result of corporate negligence. UHG has publicly confirmed that the hackers gained their initial foothold by logging into a remote access server that was not protected with multi-factor authentication (MFA). MFA is an industry-standard cyber defense that protects against hackers who have guessed or stolen a valid username and password for a system.

Testifying before the Senate Finance Committee on May 1, 2024, UHG's chief executive officer (CEO) Andrew Witty stated that UHG "policy is to have MFA for externally facing systems." But he also revealed that this industry-standard cyber defense had not been in place, company-wide, at the time of the hack, or, until the day of the hearing. Mr. Witty also revealed, in testimony the same day before the House Energy and Commerce Committee, that UHG's MFA policy did not in fact require MFA for all external servers. Instead, Mr. Witty revealed that "in certain situations where you might have, for example, older technologies which have been upgraded, you might — you may have security controls around those systems as a — as a compensatory factor." The consequences of UHG's apparent decision to waive its MFA policy for servers running older software are now painfully clear. But UHG's leadership should have known, long before the incident, that this was a bad idea.

The Federal Trade Commission (FTC) has required companies in other industries to implement MFA, among other cybersecurity best practices. The FTC has specifically required financial services companies regulated by the agency to adopt MFA, as part of the 2021 update to the Safeguards Rule. The FTC has also required several companies to use the most secure method of MFA, known as phishing-resistant MFA, in two 2022 cases, against the alcohol delivery platform Drizly and the education technology company Chegg. In both cases, the FTC held that the companies' failure to use appropriate information security practices to protect consumers' personal information was an unfair business practice that violated Section 5 of the FTC Act.

While UHG has not yet made public the full details of this incident, UHG's failure to require MFA is unlikely to be the company's only cybersecurity lapse. Hackers gaining access to one remote access server should not result in a ransomware infection so serious that the company must rebuild its digital infrastructure from scratch. UHG has not revealed how the hackers gained administrative privileges and moved laterally from that first server to the rest of the company's technology infrastructure. However, cybersecurity best practices are to have multiple lines of defense, and to wall-off the most sensitive servers in an organization, specifically to prevent this type of incident.

In addition to the company's cybersecurity failures, the company also clearly failed to plan for ransomware and to ensure that its digital infrastructure could be promptly restored in hours or days, rather than weeks. In his House testimony, Mr. Witty revealed that the company was able

to restore its cloud-based systems in a matter of days. But, Mr. Witty added, many of the company's key systems had not yet been engineered to run in the cloud. Instead, these services ran on the company's own servers, which took far longer to restore. Such a failure to adopt a resilient technology architecture demonstrates a total failure by the company to plan for and mitigate the clear, obvious risk posed by ransomware.

One likely reason for UHG's negligence, and the company's failure to adopt industry-standard cyber defenses, is that the company's top cybersecurity official appears to be unqualified for the job. Steven Martin, UHG's chief information security officer (CISO), had not worked in a full-time cybersecurity role before he was elevated to the top cybersecurity position at UHG in June, 2023, after working in other roles at UHG and Change Healthcare. Although Mr. Martin has decades of experience in technology jobs, cybersecurity is a specialized field, requiring specific expertise. Just as a heart surgeon should not be hired to perform brain surgery, the head of cybersecurity for the largest health care company in the world should not be someone's first cybersecurity job.

Due to his apparent lack of prior experience in cybersecurity, it would be unfair to scapegoat Mr. Martin for UHG's cybersecurity lapses. Instead, UHG's CEO and the company's board of directors should be held responsible for elevating someone without the necessary experience to such an important role in the company, as well as for the company's failure to adopt basic cyber defenses. The Audit and Finance committee of UHG's board, which is responsible for overseeing cybersecurity risk to the company, clearly failed to do its job. One likely explanation for this board-level oversight failure is that none of the board members have any meaningful cybersecurity expertise.

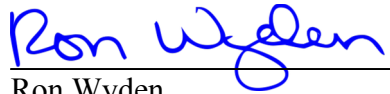
In addition to the serious harm to consumers, the health care industry, and U.S. national security, UHG's negligence has also harmed investors. The company has confirmed that it expects the breach to cost at least a billion dollars and the company has received significant amounts of negative media coverage, exposing the company to significant political risk. As the U.S. Securities and Exchange Commission (SEC) made clear in its 2022 case against SolarWinds, "[c]ybersecurity practices are important to every publicly traded company" and that "[r]easonable investors considering whether to purchase or sell SolarWinds stock would have considered it important to know the true state of SolarWinds' cybersecurity practices." The SEC also held in the Solarwinds case that companies "are required to develop reasonable safeguards against unauthorized access to Company assets by designing and maintaining reasonable controls to prevent and detect unauthorized access to, or use of, its assets."

The cyberattack against UHG could have been prevented had UHG followed industry best practices. UHG's failure to follow those best practices, and the harm that resulted, is the responsibility of the company's senior officials including UHG's CEO and board of directors. Accordingly, I urge the FTC and SEC to investigate UHG's numerous cybersecurity and

technology failures, to determine if any federal laws under your jurisdiction were broken, and, as appropriate, hold these senior officials accountable.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator
Chairman, Committee on
Finance