

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 25, 2024

Andrew Witty
Chief Executive Officer
UnitedHealth Group
P.O. Box 1459
Minneapolis, MN 55440-1459

Dear Mr. Witty:

We write to request information about a cybersecurity incident and the subsequent extended system outages at UnitedHealth Group-owned (UHG) Change Healthcare, a “software and data analytics” firm providing prescription, administrative, and payment processing services across the U.S. health care system.¹ Change Healthcare reportedly handles medical records for one in three patients in the United States, and provides services to external clients and customers, as well as subsidiaries of UHG—the nation’s health insurance market leader with a 28% market share.² Given your company’s dominant position in the nation’s health care and health insurance industry, Change Healthcare’s prolonged outage as a result of the cyberattack has already had “significant and far-reaching” consequences for patients, physicians, and thousands of hospitals, pharmacies and medical practices, and is disrupting patients’ timely access to affordable medication and treatments.³

According to Change Healthcare incident reports, the company faced “enterprise-wide connectivity” problems in the morning of February 21, 2024.⁴ Several hours later, the company

¹ UnitedHealth Group, *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform* (Jan. 6, 2021) (online at www.unitedhealthgroup.com/newsroom/2021/2021-01-06-optuminsight-and-change-healthcare-combine.html). Change Healthcare is owned by UnitedHealth Group (UHG) through Optum—UHG’s “information and technology-enabled health services” firm. U.S. Securities and Exchange Commission, *UnitedHealth Group (Form 10-K)* (online at www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/0000731766/000073176624000081/unh-20231231.htm) (accessed Mar. 8, 2024).

² American Medical Association, *AMA Identifies Market Leaders in Health Insurance* (Dec. 12, 2023) (online at www.ama-assn.org/press-center/press-releases/ama-identifies-market-leaders-health-insurance).

³ *Change Healthcare Cyberattack Having “Far-Reaching” Effects on Providers*, Healthcare Dive (Mar. 1, 2024) (online at www.healthcaredive.com/news/change-healthcare-cyberattack-unitedhealth-group-provider-impact/708950/).

⁴ Optum, *Incident Report for Optum Solutions* (online at <https://status.changehealthcare.com/incidents/hqpjz25fn3n7>) (accessed Mar. 4, 2024).

stated that it was “experiencing a network interruption related to a cyber security issue.”⁵ The next day, UHG filed a report with the Securities and Exchange Commission, stating that a “cyber security threat actor had gained access to some of the Change Healthcare information technology systems.”⁶ Concurrently, Change Healthcare reported that “once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact.”⁷ It appears that Change Healthcare’s pharmacy, payments, and claims systems were disconnected or diverted for nearly one month.⁸

Your company’s rapid consolidation and vertical integration of its health care networks, including the expansion of UHG-owned primary care providers and specialty pharmacies, have significant consequences for the nation’s health care system.⁹ UHG’s acquisition of Change Healthcare has increased Change Healthcare’s control of the health information technology systems environment market, allowing the company to process transactions and touch patient care in 90% of all U.S. hospitals, 80% of all U.S. health plans, and more than 67,000 U.S.-based retail and military pharmacies.¹⁰

Roughly 725 data breaches within the U.S. health care system were reported in 2023—a 162% increase in the last decade.¹¹ The rising number of cyberattacks against the U.S. health care system, especially against an actor that holds outsized influence on the market, poses a clear and present threat to national security and public health. In response, U.S. federal agencies have repeatedly issued guidance to the industry to ensure U.S. health care systems have the appropriate tools and mitigation measures to prevent cyberattacks. For example, on December

⁵ *Id.*

⁶ U.S. Securities and Exchange Commission, *UnitedHealth Group Incorporated (Form 8-K)* (online at www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm) (accessed Mar. 4, 2024). Ransomware group ALPHV/Blackcat has since claimed responsibility for the February 2024 cyberattack against Change Healthcare. *Ransomware Group Blackcat is Behind Cyberattack on UnitedHealth Division, Company Says*, CNBC (Feb. 29, 2024) (online at www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html).

⁷ Optum, *Incident Report for Optum Solutions* (online at <https://status.changehealthcare.com/incidents/hqjz25fn3n7>) (accessed Mar. 4, 2024).

⁸ *Id.*; UnitedHealth Group, *Information on the Change Healthcare Cyber Response* (updated Mar. 14, 2024) (online at www.unitedhealthgroup.com/changehealthcarecyberresponse); UnitedHealth Group, *UnitedHealth Group Update on Change Healthcare Cyberattack* (Mar. 7, 2024) (online at www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html).

⁹ See *How UnitedHealth Group Grew Bigger Than the Nation’s Biggest Banks*, CNBC (May 20, 2023) (online at www.cnbc.com/2023/05/20/how-unitedhealth-group-grew-bigger-than-the-nations-biggest-banks.html).

¹⁰ *Hospitals and Pharmacies Reeling After Change Healthcare Cyberattack*, Wall Street Journal (Feb. 23, 2024) (online at www.wsj.com/articles/hospitals-urged-to-disconnect-from-unitedhealths-hacked-pharmacy-unit-11c9691e). See also Department of Justice, *Justice Department Sues to Block UnitedHealth Group’s Acquisition of Change Healthcare* (Feb. 24, 2022) (online at www.justice.gov/opa/pr/justice-department-sues-block-unitedhealth-group-s-acquisition-change-healthcare); *U.S. Opens UnitedHealth Antitrust Probe*, Wall Street Journal (Feb. 27, 2024) (online at www.wsj.com/health/healthcare/u-s-launches-antitrust-investigation-of-healthcare-giant-unitedhealth-ff5a00d2).

¹¹ The HIPAA Journal, *Healthcare Data Breach Statistics* (online at www.hipaajournal.com/healthcare-data-breach-statistics/) (accessed Mar. 4, 2024).

19, 2023, the Department of Health and Human Services (HHS), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency (CISA) issued a Joint Cybersecurity Advisory that emphasized key indicators of compromise and techniques by ransomware group ALPHV/Blackcat—the entity that has claimed responsibility for the attack on Change Healthcare.¹² However, the Committee is concerned that UnitedHealth Group is restricting the ability of federal agencies to provide applicable assistance to Change Healthcare—a company cited by CISA as a “lynchpin in claims processing, medical claims, and prior authorization for the nationwide healthcare system.”¹³ For example, CISA stated to Committee staff in a March 13, 2024, briefing that the agency is “handcuffed in this instance because of the lack of transparency and lack of information flowing into us [from UnitedHealth Group/Change Healthcare].”¹⁴

Pharmacies are confronting interruptions to processing prescription insurance claims, and small- and medium-sized hospitals that depend on Change Healthcare claims and billing services have found themselves in financial distress as a result of the extended outages. Following the shutdown of Change Healthcare’s system environment, U.S.-based retail and military pharmacies, as well as hospital networks, that you serve began reporting significant processing delays and ongoing interruptions for prescription claims, billing, and other administrative activities through Change Healthcare-offered technology solutions.¹⁵ For example, the President of the Healthcare Association of New York State said its networks had difficulty “verify[ing] patient eligibility and coverage ... communicat[ing] pharmacy prescription...fil[ing] claims...and receiv[ing] normal cash flow to support operations.”¹⁶ TRICARE—the U.S. military’s health care system supporting active duty servicemembers and their families and veterans—indicated the system shutdown disrupted “all military pharmacies worldwide and some retail pharmacies nationally.”¹⁷ The American Hospital Association (AHA) stated on February 29, 2024, that in addition to prescription processing delays, “hospitals are having issues

¹² Cybersecurity and Infrastructure Security Agency, #StopRansomware: *ALPHV Blackcat* (revised Feb. 27, 2024) (online at www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a). See also *Ransomware Group Blackcat is Behind Cyberattack on UnitedHealth Division, Company Says*, CNBC (Feb. 29, 2024) (online at www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html).

¹³ Briefing by Cybersecurity Infrastructure and Security Agency, to Staff, Committee on Oversight and Accountability (Mar. 13, 2024).

¹⁴ *Id.*

¹⁵ See e.g., *Hospitals and Pharmacies Reeling After Change Healthcare Cyberattack*, Wall Street Journal (Feb. 23, 2024) (online at www.wsj.com/articles/hospitals-urged-to-disconnect-from-unitedhealths-hacked-pharmacy-unit-11c9691e); *Cybersecurity Breach at UnitedHealth Subsidiary Causes Rx Delays for Some Pharmacies* (Feb. 22, 2024) (online at www.cbsnews.com/news/cybersecurity-issue-united-health-change-healthcare-pharmacies-prescription-delays/).

¹⁶ *A Large U.S. Health Care Tech Company Was Hacked. It’s Leading to Billing Delays and Security Concerns*, Washington Post (Feb. 29, 2024) (online at www.washingtonpost.com/health/2024/02/29/change-cyberattack-hospitals-pharmacy-alphv-unitedhealthcare/ab2d4e6c-d74a-11ee-82ad-c2391b06a8f5_story.html).

¹⁷ TRICARE, *Change Healthcare Cyberattack Impact on MHS Pharmacy Operations* (Feb. 22, 2024) (online at <https://newsroom.tricare.mil/News/TRICARE-News/Article/3684541/change-healthcare-cyberattack-impact-on-mhs-pharmacy-operations>).

processing claims, billing patients and checking insurance coverage for care,” and this cyberattack “could affect the ability to pay workers and buy medicine and supplies.”¹⁸

Your company’s efforts to disconnect Change Healthcare’s systems in response to the February 2024 cyberattack appears to have disrupted patients’ timely access to affordable medication and interrupted crucial elements of our health care system. Patients who rely on life-saving medications may have to choose between paying high out-of-pocket prescription medication costs, devote significant time and resources to finding affordable alternatives, or delay obtaining their medication altogether if their pharmacy’s billing and coverage services were disrupted as a result of the cyberattack. For example, insured patients who depend on migraine medication Treximet could see their next prescription refill costs increase from \$16 to \$1,338 for nine tablets.¹⁹ According to Kaiser Family Foundation, 60% of uninsured adults reported “they have skipped or postponed getting health care they needed due to cost,” and insured patients could face similar cost concerns as claims processing disruptions continue.

To help us understand the scope and extent of the Change Healthcare cybersecurity breach and subsequent system outages, and the steps your company is taking to remedy disruptions identified within the system environment, please provide written responses to the following questions, and provide a staff briefing on this incident, no later than April 8, 2024:

1. When did Change Healthcare first notify its clients, customers, and/or partners (including UnitedHealth Group subsidiaries) of the February 2024 cyberattack, and by what method(s) was this information communicated?
2. What specific Change Healthcare systems and/or system infrastructure were directly disrupted or targeted by the threat actor during the February 2024 cyberattack?
3. What types of data and/or information (including types of personally identifiable information (PII) and protected health information (PHI)) were compromised by the February 2024 cyberattack?
4. How many PII records and PHI were compromised as a result of the February 2024 cyberattack? Please specify the extent to which records from Medicare, Medicaid, and TRICARE beneficiaries were compromised as a result of the cyberattack.
5. What efforts have been made to report to and coordinate with HHS, FBI, and CISA following the February 2024 cyberattack against Change Healthcare?

¹⁸ *A Large U.S. Health Care Tech Company Was Hacked. It’s Leading to Billing Delays and Security Concerns*, Washington Post (Feb. 29, 2024) (online at www.washingtonpost.com/health/2024/02/29/change-cyberattack-hospitals-pharmacy-ahv-unitedhealthcare/ab2d4e6c-d74a-11ee-82ad-c2391b06a8f5_story.html).

¹⁹ GoodRx, *Treximet* (online at www.goodrx.com/treximet/medicare-coverage) (accessed Mar. 4, 2024); Drugs.com, *Treximet Prices, Coupons and Patient Assistance Programs* (online at <https://www.drugs.com/price-guide/treximet>) (accessed Mar. 4, 2024).

6. Change Healthcare reportedly disconnected affected system(s) as early as February 22, 2024, before restoring pharmacy processing and payments services by March 15, 2024, and testing connectivity of medical claims by March 18, 2024.²⁰
 - a. What Change Healthcare systems and/or software were disconnected in response to the February 2024 cyberattack? Please include the current status of all affected systems and when Change Healthcare anticipates restoring all disconnected systems.
 - b. What were the deciding factor(s) driving Change Healthcare’s decision to shut off its system(s)?
 - c. How did Change Healthcare mitigate risks to all affected clients, customers, and/or partners (e.g., pharmacies, hospitals, provider networks, and patients) when it shut off the affected system(s)?
7. What steps has Change Healthcare taken to isolate the affected system(s) and restore the system environment involved in the February 2024 cyberattack?
8. UHG has reportedly begun offering financial resources to affected clients, customers, and partners, including by establishing a “Temporary Funding Assistance Program” through its subsidiary Optum.²¹
 - a. What types of providers or entities are eligible for funding relief through the Temporary Funding Assistance Program (the Program)?
 - b. What factors or criteria does Optum review and assess to estimate funding relief for eligible participants through the Program?
 - c. What is the average funding disbursement for an eligible participant to receive payments through the Program?
9. What additional steps has Change Healthcare taken to assist all clients, customers, and partners whose systems, services, or cash flow have been disrupted as a result of the February 2024 cyberattack and subsequent restoration efforts?

²⁰ UnitedHealth Group, *Information on the Change Healthcare Cyber Response* (updated Mar. 18, 2024) (online at www.unitedhealthgroup.com/ns/changehealthcare.html).

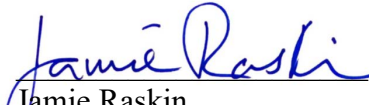
²¹ Optum, *Expanded Temporary Funding Assistance Program for Providers* (online at www.optum.com/en/business/providers/health-systems/payments-lending-solutions/optum-pay/temporary-funding-assistance.html) (accessed Mar. 8, 2024); American Hospital Association, *AHA Expresses Concern with UHG Program in response to Cyberattack on Change Healthcare* (Mar. 4, 2024) (online at www.aha.org/lettercomment/2024-03-04-aha-expresses-concerns-uhg-program-response-cyberattack-change-healthcare).

10. Were you aware of government cybersecurity alerts and advisories about rising ransomware attacks against U.S. health care systems, including but not limited to the December 19, 2023, Joint Cybersecurity Advisory titled “#StopRansomware: ALPHV Blackcat”?
 - a. If yes, what steps did Change Healthcare take to respond to these federal alerts and advisories, and strengthen consumer privacy and cybersecurity measures, prior to the February 2024 cyberattack?
11. What guidance, policies, and/or procedures does Change Healthcare have in place, related to consumer privacy and cybersecurity, to prevent and/or thwart cyberattacks?
12. What additional measures has the company taken, if any, to improve consumer privacy and cybersecurity measures in light of the February 2024 cyberattack?

The Committee on Oversight and Accountability is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

An attachment to this letter provides additional instructions for responding to this request. If you have any questions regarding this request, please contact Democratic Committee staff at (202) 225-5051.

Very truly yours,


Jamie Raskin
Ranking Member

Enclosure

cc: The Honorable James Comer, Chairman