UNITEDHEALTH GROUP

Testimony of Andrew Witty
Chief Executive Officer, UnitedHealth Group
Before the House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
"*Examining the Change Healthcare Cyberattack*"
May 1, 2024

Introduction

Good afternoon, Chairman Griffith, Chair Rodgers, Ranking Member Castor, Ranking Member Pallone and Members of the Subcommittee. Thank you for the opportunity to testify here today. My name is Andrew Witty. I serve as chief executive officer of UnitedHealth Group, a health care and well-being company founded 50 years ago in Minnesota.

Our mission is to help people live healthier lives and help make the health system work better for everyone. My colleagues include doctors, nurses, engineers, scientists – experts and caregivers in nearly every discipline of modern medicine.

Together, we are working to help enable our health system's transition to value-based care and are empowering physicians and their care teams to deliver more personalized, high-quality care that delivers better outcomes at a lower cost.

We pursue these objectives through our two distinct and complementary businesses, UnitedHealthcare and Optum.

UnitedHealthcare provides a full range of health benefits, serving individuals, small businesses, large companies, labor unions, universities and hospitals. More seniors choose our Medicare Advantage offerings, and more employers choose our benefits plans than any other company. And we partner with more than 30 states to serve individuals and families through Medicaid.

Optum offers a full spectrum of health services, bringing together clinical expertise, technology and data to advance integrated, patient-centered care; make clinical, administrative and financial processes simpler and more efficient; and connect patient care across the continuum, including pharmacy, medical and behavioral care.

Change Healthcare is now part of Optum, and works across the health system to enable information, claims and payments to flow quickly and accurately between physicians, pharmacists, health plans and governments.

Today's Hearing

I appreciate the Committee's interest in the recent cyberattack on Change Healthcare. The cyberattack was unprecedented, as the criminals who perpetrated it caused incredible disruption across the health care system.

From pharmacists having to manually submit claims to the rural family medicine practice struggling to make payroll – the impacts of an attack by organized criminals, no matter how temporary, were real.

As a result of this malicious cyberattack, patients and providers have experienced disruptions and people are worried about their private health data. To all those impacted, let me be very clear: I am deeply sorry.

From the moment I learned of the intrusion, I felt a profound sense of responsibility to do everything we could to preserve access to care and support our customers and clients. Our

response and reaction to this attack has been grounded in three principles: to secure the systems; to ensure patient access to care and medication; and to assist providers with their financial needs.

We have been working 24/7 from the day of the incident and have deployed the full resources of UnitedHealth Group on all aspects of our response and restoration efforts. I want this Committee and the American public to know that the people of UnitedHealth Group will not rest – I will not rest – until we fix this.

We know there is more to be done, and we appreciate the ongoing efforts of our customers, employees and government partners – especially CMS and HHS – who have offered great support as we continue these efforts together.

Cyberattacks continue to increase in frequency and significance, with one analysis calculating that in 2023, cybercriminals collected an all-time high of over $1 billion in ransom.[1] Our company alone repels an attempted intrusion every 70 seconds – thwarting more than 450,000 intrusions per year. These criminals continue to adapt and develop more sophisticated and malicious methodologies, and they have increasingly targeted critical infrastructure, including schools, government agencies and the health care sector. These adversaries are willing to attack everything from community hospitals to pharmacies to networks like ours that enable the information exchange necessary to provide care.

I would not wish a cyberattack on anyone. That is one reason why, as chief executive officer of UnitedHealth Group, I have strongly committed our organization to work with law enforcement,

[1] Chainalysis, *The 2024 Crypto Crime Report*, at 11 (Feb. 2024), https://bit.ly/49TCvQ5.

policy makers and industry participants to help prepare for and recover from the impact of the hundreds of other attacks that continue to be perpetrated across so many facets of America's critical infrastructure each year, and to collectively strengthen our cybersecurity resiliency to these evolving threats.

The Ransomware Attack

On the morning of February 21, a cybercriminal calling themselves ALPHV or BlackCat deployed a ransomware attack inside Change Healthcare's information technology environments, encrypting Change's systems so we could not access them.

Our response was swift and forceful. Not knowing the entry point of the attack at the time, we immediately severed connectivity with Change's data centers to eliminate the potential for further infection. While shutting down many Change environments was extremely disruptive, it was the right thing to do.

We secured the perimeter of the attack and prevented malware from spreading beyond Change to the broader health system.

It worked. There has never been any evidence of spread beyond Change – not to any external environment and not to Optum, UnitedHealthcare or UnitedHealth Group.

Within hours of the ransomware launch, we contacted the FBI and remain in regular communication. We shared critical information, including details about the intrusion, the method of attack, Indicators of Compromise (IOC) and other information that would assist in their investigation. We are grateful for the FBI's work on this matter and the support they have provided,

and we will continue to share information that will enable law enforcement to pursue, capture and bring these criminals to justice.

We are working tirelessly to uncover and understand every detail we can, which we will use to make our cyber defenses stronger than ever. We are committed to sharing accurate answers safely, appropriately and responsibly.

Cyber experts continue to investigate the incident. While we will learn more and our understanding may change, here's what I can share today. On February 12, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops. The portal did not have multi-factor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed nine days later.

As we have addressed the many challenges in responding to this attack, including dealing with the demand for ransom, I have been guided by the overriding priority to do everything possible to protect peoples' personal health information.

As chief executive officer, the decision to pay a ransom was mine. This was one of the hardest decisions I've ever had to make. And I wouldn't wish it on anyone.

Protecting Patient Data

As we continue our investigative efforts, we are also working to understand the full scope of impacted patient, provider and payer information. As we have previously confirmed, based on initial targeted data sampling to date, we found files containing protected health information (PHI) and personally identifiable information (PII), which could cover a substantial proportion of people

in America. So far, we have not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.

Given the ongoing nature and complexity of the data review, it is likely to take several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals, partly because the files containing that data were compromised in the cyberattack. Our teams, along with leading external industry experts, continue to monitor the internet and dark web to determine if data has been published.

We will, of course, comply with legal requirements and provide notice to affected individuals, and have offered to our customers and clients to provide notice on their behalf where it is permitted. We are working closely with HHS's Office of Civil Rights to make sure our notice is effective, useful and complies with the law.

Rather than waiting to complete this review, we are providing free credit monitoring and identity theft protections for two years, along with a dedicated call center staffed by clinicians to provide support services. Anyone concerned their data may have been impacted should visit changecybersupport.com for more information.

Our Response and Restoration Progress

We continue to make substantial progress in restoring Change Healthcare's impacted services, guided first and foremost by our commitment to protect personal information and the three principles I spoke of earlier: to secure the systems; to ensure patient access to care and medication; and to assist providers with their financial needs.

1. **Securing the Systems and Restoring them Safely**

As I noted, we promptly severed connectivity to the Change environments and established a perimeter, thereby quarantining the threat and preventing further damage.

By the afternoon of February 21, experts from Google, Microsoft, Cisco, Amazon and others were enroute to Change's Nashville Central Command Operations Center, where they joined security teams from Mandiant and Palo Alto Networks. We are exceedingly grateful for their support.

Together with our Change Healthcare colleagues, they immediately began the around-the-clock and enormously complex task of safely and securely rebuilding Change Healthcare's technology infrastructure from the ground up. The team replaced thousands of laptops, rotated credentials, rebuilt Change Healthcare's data center network and core services, and added new server capacity. The team delivered a new technology environment in just weeks – an undertaking that would have taken many months under normal circumstances.

2. **Ensuring Patients' Access to Needed Care**

We have prioritized our restoration efforts on systems and networks that are most critical to access to care: pharmacy, provider payments and claims.

Pharmacy Services: So that we could ensure, as much as possible, continued access to medication, we immediately prioritized restoring our pharmacy networks to be certain that patients could get the prescriptions they needed. By March 7, 99% of pre-incident pharmacies were able to process claims, and today, it is just a fraction of a percent below normal service levels.

Medical Claims: Medical claims across the health system are now flowing at near normal levels as systems come back online or providers switch to other methods of submission. We realize there are a small number of providers who continue to be adversely impacted. We are working with them to find alternative submission solutions and will continue to provide them with financial support as needed.

Payments: Payment processing by Change Healthcare, which represents about 6% of all payments, is at approximately 86% of pre-incident levels and is increasing as additional functionality is restored.

3. **Payer and Provider Support**

In the days after the ransomware attack, we worked quickly to find alternative channels or workarounds for payers and providers within the networks facilitating the near-instant transmission of information across the health system so that transactions could flow. This involved pushing volume to Change Healthcare's competitors to allow the system to regain functionality as quickly as possible, and we are grateful for their assistance.

We also immediately recognized that many providers would be affected by the disruption in claims and payments flows, so we worked quickly to get funds into the hands of providers who need it.

To this end, UnitedHealthcare accelerated more than a billion dollars in claims payments to immediately infuse providers with liquidity.

For claims not covered by UnitedHealthcare, we set up a Temporary Funding Assistance Program offering no-cost, no-interest loans to any provider who needed it. We harnessed the strength of our nationwide payments network – the same network we used in 2020, during the pandemic – to disburse billions of dollars in a matter of days of federal CARES Act funding to providers on behalf of HHS.

As of last Friday, April 26, UnitedHealth Group has advanced more than $6.5 billion in accelerated payments and no-interest, no-fee loans to thousands of providers. About 34% of these loans have gone to safety net hospitals and federally qualified health centers that serve many of the patients and communities at the highest risk. While some of our early estimates of providers' potential gaps did not address their full need given our lack of visibility into their claims flow, we quickly adjusted.

We are committed to providing this financial assistance for providers for as long as it takes to get their claims and payments flowing at pre-incident levels. If there are providers or payers in your states who need help, please put us in touch with them. We pledge to do everything in our power to fix their system or underwrite their cashflow, simple as that.

Policy Solutions

The Change Healthcare attack demonstrates the growing need to fortify cybersecurity in health care. I look forward to working with policymakers and other stakeholders to bring our experience to bear in helping develop strong, practical solutions.

We support mandatory minimum security standards – developed collaboratively by the government and private sector – for the health care industry. Importantly, these efforts must

include funding and training for institutions that need help in making that transition, such as hospitals in rural communities.

We also support efforts to strengthen our national cybersecurity infrastructure, including greater notification to law enforcement and standardized and nationalized cybersecurity event reporting.

Conclusion

In closing, I want to say again to all those impacted, I am deeply sorry.

I also want to express my sincerest thanks to our customers, who along with so many of our colleagues stepped up to help our health system continue to serve all who depend on it during this difficult time. And I would like to extend my appreciation to our partners in government and in the private sector for the tremendous assistance they have provided throughout.

Fighting cybercrime is an enormous task and one that requires us all – industry, law enforcement and policymakers – to come together.

I look forward to answering your questions today and to sharing our learnings so that everyone can better protect themselves from future attacks.

###