Responses to Questions for the Record for Andrew Witty

U.S. Senate Committee on Finance
Full Committee Hearing
Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next

1. **You testified that UHG had a policy, before the hack, requiring multi factor authentication for externally facing systems. You also testified that the server that was initially hacked did not have MFA enabled.**

    - **Was that server in violation of your MFA policy, or did UHG's policy permit legacy external servers to not utilize MFA?**

Response:

UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally-facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

2. **Please detail the steps taken by UHG and Change Healthcare, prior to the hack, to plan for ransomware, including to ensure that the company could quickly restore IT services if the company needed to rebuild its infrastructure from scratch.**

Response:

UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the Company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the Chief Digital and Technology Officer and Chief Information Security Officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response

comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

To ensure we are constantly assessing and improving our capabilities, we collaborate closely with key technology partners to mutually share information about cybersecurity threats and best practices. Additionally, we retain and employ services from external security firms to review our operating capabilities, enhance our strategic plans, and provide immediate, force-multiplying rapid-response and forensics services.

3. **Please identify the steps taken by UHG's board of directors, in the two years before the hack, to assess the company's exposure to ransomware, and to ensure that the company had mitigated this source of cyber risk.**

Response:

UHG has a deeply experienced board of directors who oversee the program and bring broad-based skills in risk management, including cybersecurity. UHG's Audit and Finance Committee oversees cybersecurity risks, and the members have experience with organizations that face significant cybersecurity risks.

The UHG Board stays up-to-date on the threat posed by ransomware, specifically, through recurring cybersecurity reports delivered by UHG's Enterprise Information Security (EIS) team. These reports emphasize the significance of the threat posed by ransomware attacks (particularly in relation to health care organizations) and outline UHG's efforts to combat this threat in the areas of prevention, detection, and response. In addition, the Audit and Finance Committee covers cybersecurity as a topic at each regularly-scheduled quarterly meeting.

Mandiant now serves as an advisor to the Audit and Finance Committee of the Board. Cybersecurity is already a standing agenda item, and Mandiant will have a seat at the table going forward for those discussions. Mandiant has a deep knowledge of the company, along with broad knowledge and visibility of threats facing the health care industry.

4. **Did the ransomware deployed against Change Healthcare's systems only infect systems running Microsoft Windows, or did it also infect systems running other operating systems?**

Response:

The ransomware deployed by the threat actor infected Change Healthcare's Windows and ESXi systems.

5. **Did the hackers gain access to Change Healthcare's "Tier 0" servers, including the company's Active Directory server, which is used to centrally manage accounts across an enterprise?**

    - **If yes, please detail the steps the hackers took to gain access to and control of these high-value servers.**

Response:

The threat actor gained access to Change Healthcare's Active Directory server after using privilege escalation techniques.

6. **In response to a question from the Chairman about whether the hackers stole data pertaining to US government employees, Mr. Witty testified that "what we've been able to identify is indeed that a substantial proportion of people across the country's data could be implicated here. We do believe there will be members of the armed forces or and the Veterans…." Mr. Witty also said he would prioritize providing in writing an assessment of the number of military personnel affected. It has been over a week since the hearing:**

    - **How many Americans had their data stolen?**
    - **How many US government employees had their data stolen?**
    - **How many members of the US military had their data stolen?**
    - **What was the nature of the medical, financial, and other information stolen?**

Response:

Based on initial targeted data sampling to date, the Company has found files containing protected health information ("PHI") or personally identifiable information ("PII"), which could cover a substantial proportion of people in America. Based on this limited sampling, it appears that the exfiltrated data includes transactional claims data, which may involve details about treatments, payments, and balances. Any PHI or PII impacted by the cyberattack will likely vary by individual. For example, depending upon the circumstances, the data may include health insurance member numbers, diagnostic and treatment codes, and provider identities, as well as payments and balances. There may also be PII, such as full names, dates of birth, addresses, social security numbers, or other types of data. At this time, we have not seen evidence of exfiltration of more detailed materials like doctors' charts or medical histories among the data, which could change based on the ongoing investigation.

Given the ongoing nature and complexity of the data review, it will take additional analysis before enough information will be available to identify specific impacted customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

7. **According to your testimony, "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." That was over 12 weeks ago. Under the Health Insurance Portability and Accountability Act, Change Healthcare is responsible for notifying the Secretary (through the Office of Civil Rights breach portal) if it is a covered entity or the relevant covered entity or business associate of a breach within 60 days of the discovery of a breach.**

    - **In your role as a covered entity and business associate, have you notified other covered entities or business associates?**
    - **Have you notified the Secretary officially with a breach report as required by HIPAA? If not, by what date will UnitedHealth Group submit a breach notification to the Department of Health and Human Secretary Office of Civil Rights?**
    - **By what date will UnitedHealth Group notify the millions of Americans impacted by this breach?**

Response:

UHG is continuing our discussions with the HHS Office for Civil Rights about how appropriate notice can be made to regulators, customers, and affected individuals, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

UHG is working as quickly as possible to develop a complete and accurate assessment of the individuals impacted by this cyberattack. Given the ongoing nature and complexity of the Company's data review, the Company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack. The process of analyzing the dataset that was made available to the Company by the FBI is complex and requires significant compute resources because it requires unpacking and unzipping many layers of files within the dataset in order to identify the individuals whose data may be impacted. This takes time, and it must be done extremely methodically. UHG is working as quickly and accurately as possible and will keep the Committee and the public posted on its progress.

UHG is not waiting to complete its data review and notifications—the Company is offering a robust set of protections and support services to any individual concerned that they are affected. These services include free credit monitoring and identity theft protections for two years and a dedicated call center that can connect individuals with trained clinicians. Any individual concerned that their data has been impacted should visit changecybersupport.com or

call 1-866-262-5342 to find more details regarding the support services that UHG is making available.

8. **Beyond 2 years of credit and identity monitoring, what will UnitedHealth Group offer to compensate the patients who had their care disrupted and information stolen?**

Response:

In addition to free credit monitoring and identity theft protections for two years, UHG has also created a dedicated call center staffed by clinicians to provide support services. Any individual concerned that their data has been impacted should visit www.changecybersupport.com or call 1-866-262-5342 to find more details regarding the support services that UHG is making available.

The company, along with leading external industry experts, continues to monitor the internet and dark web to determine if data has been published. There were 22 screenshots, allegedly from exfiltrated files, some containing PHI and PII, posted for about a week on the dark web by a malicious threat actor. No further publication of PHI or PII has occurred at this time. To date, the Company has not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.

Furthermore, through Optum Rx, UHG notified network pharmacy partners and pharmacy associations that we would reimburse all appropriate pharmacy claims filled with the good faith understanding that a medication would be covered. For patients who could not use their coupons during the Change Healthcare outage, the Company has been and will continue to contact those patients and honor their coupons to ensure that the patients are reimbursed for their out-of-pocket medication expenses.

9. **Beyond Optum's Temporary Funding Assistance Program for Providers, what will UnitedHealth Group offer to compensate providers who have had to incur greater business expenses and worry because of this breach?**

Response:

The Company's restoration and remediation efforts focused on protecting patients and helping providers, and the Company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. As of May 15, approximately $7 billion has been advanced to providers, with 34% of the total funds getting routed to safety net hospitals and federally qualified health centers serving many of the patients and communities at the highest risk. More than 14,000 unique Taxpayer Identification Numbers (TINs) have received funds through the temporary funding program.

To the extent providers have incurred other costs associated with the attack, UHG is committed to reviewing their issues and working to resolve their concerns on a case-by-case basis.

10. Which external companies performed Change Healthcare's HITRUST audits over the past five years, and did these audits identify Change Healthcare's failure to use MFA?

Response:

The HITRUST Framework (HITRUST CSF) provides a comprehensive approach to managing cybersecurity risks related to sensitive data and assuring regulatory compliance. Organizations across sectors use this common security framework to evaluate their security posture. UHG leverages the HITRUST CSF framework, among other things, to measure the company's standard of security maturity, prioritize future enhancements, and improve its security controls over time through continuous monitoring and assessment. UHG maintains HITRUST CSF certifications across many of its applications, including certain of Change Healthcare's systems. These standards provide sophisticated risk frameworks that UHG applies to many different aspects of its business. UHG works diligently and on an ongoing basis to implement these frameworks, including their risk management controls, and to ensure that its security protocols meet or exceed these standards. Both UHG and Change Healthcare have had regular assessments by external and internal parties.

11. Why was Change Healthcare's backup infrastructure not segregated from the rest of the company's infrastructure, which would have prevented the ransomware from also infecting the backup systems?

- **Had this issue been identified by any previous audits?**

Response:

UHG had significant contingency and backup infrastructure across UHG's systems in place prior to the incident. Beyond backups, critical Change Healthcare services had redundancy across servers and across separate datacenters. That redundancy is designed to ensure continuity of the service in the event a single server or single data center goes off-line. The ransomware deployed by the threat actors affected many of Change Healthcare's systems. At the time of the incident, UHG was in the process of upgrading some of Change Healthcare's systems, including primary and redundant servers.

To be clear, after the incident, Change Healthcare was able to use backups dated prior to the incident. Those backups were used to restore service in an environment that was newly-built after the incident, in order to be certain that the new systems would be clean and safe for use by the Company and clients. This took significant investment and effort across the UHG enterprise, as returning each service to production required key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, and validation.

In a matter of weeks, UHG had replaced thousands of Change Healthcare laptops, rotated credentials, rebuilt the data center network and core services, and added new server capacity. UHG effectively built a brand-new functioning data center and workforce. In addition, UHG reissued around 11,000 clean devices to Change Healthcare employees and contractors, the

majority of which were delivered globally over a two-week period. At the same time, UHG was able to use Optum's back-up system to help some providers carry on without interruption. UHG also rerouted some clients to competitors after the incident and is now encouraging clients to have at least two alternative channels in case of any future interruptions.

12. **Last month, I wrote to the Department of Health and Human Services Secretary Becerra regarding protecting critical infrastructure within the health care sector. In that letter, I highlighted the need for a strong relationship between public and private partners to ensure the safety of U.S. critical infrastructure systems. I also inquired about legacy information technology systems. Cyberattacks on our health care system not only have severe impacts on the United States economy but put lives at risk.**

    - **Has UnitedHealth Group taken every available action to immediately remove memory safety risks in its IT and software?**

Response:

UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the Company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the Chief Digital and Technology Officer and Chief Information Security Officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

13. My understanding is Change Healthcare touches one in three medical records in the United States. I would like to better understand how Change Healthcare stores and manages patient data.

- **How does Change Healthcare manage and store patient data?**
- **Where is the data stored?**
- **Is it stored by a third-party?**
- **At any point through processing, coding, storing, etc. is patient data ever sent overseas? Please be more specific than what you provided at the hearing.**

Response:

UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. UHG's framework allows the Company to identify, assess, and mitigate the risks, and assists UHG in revising its policies and proactive safeguards to protect its systems and customer and patient information.

UHG and its subsidiaries rely in certain circumstances on third-party service providers to process, store, and transmit data and information. It may be stored on servers owned and managed by UHG or by third-party vendors, or in cloud services owned and managed by third-party vendors.

UHG requires third-party service providers to handle data and information in accordance with its data privacy and information security requirements and applicable federal and state laws. U.S. customer data may be processed or accessed outside the United States in accordance with UHG's data protection policies. Accordingly, UHG engages with its third-party service providers to identify and remediate vulnerabilities, to monitor system upgrades to mitigate future risk, and to understand that the third-party service providers employ appropriate and effective controls and continuity plans for their systems and operations.

14. According to the Federal Bureau of Investigation, there were 249 ransomware attacks against the health care industry in 2023.

- **Has UnitedHealth Group experienced another cyberattack since February 21? You indicated during the hearing you would have to get back to me, so please provide more specifics.**

We are not aware of another ransomware attack after the attack claimed on February 21, 2024 by the ALPHV/BlackCat Group.

15. **Has any state or federal agency asked you not to publicly discuss Blackcat/AlphV's access to protected health information? If so, who?**

Response:

Within hours of the ransomware launch, we began cooperating closely with law enforcement, and we continue to work with state and federal agencies to respond to the attack. We are not aware of any state or federal agency asking any individual at UHG to withhold information from patients and providers about potentially compromised protected health information.

16. **According to the Wall Street Journal, Blackcat/AlphV was operating from February 12, 2024, to February 21, 2024, without any knowledge by Change Healthcare.**

    - **How many days did Blackcat/AlphV have access to protected health information?**

Response:

On February 12, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops or applications. Between February 17–20, 2024, the threat actor exfiltrated protected health information from Change Healthcare's systems.

17. **UnitedHealth Group said it will "likely take several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals." HIPAA Breach Notification Rules require individuals must be notified without unreasonable delay and at minimum within 60 days of the breach discovery.**
    - **Why the delay?**
    - **What do you expect patients potentially affected to do right now?**

Response:

UHG is continuing our discussions with the HHS Office for Civil Rights about how appropriate notice can be made to regulators, customers, and affected individuals, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

UHG is working as quickly as possible to develop a complete and accurate assessment of the individuals impacted by this cyberattack. Given the ongoing nature and complexity of the Company's data review, the Company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack. The process of analyzing the dataset that was made available to the Company by the FBI is complex and requires significant compute resources because it requires unpacking

and unzipping many layers of files within the dataset in order to identify the individuals whose data may be impacted. This takes time, and it must be done extremely methodically. UHG is working as quickly and accurately as possible and will keep the Committee and the public posted on its progress.

UHG is not waiting to complete its data review and notifications—the Company is offering a robust set of protections and support services to any individual concerned that they are affected. These services include free credit monitoring and identity theft protections for two years and a dedicated call center that can connect individuals with trained clinicians. Any individual concerned that their data has been impacted should visit www.changecybersupport.com or call 1-866-262-5342 to find more details regarding the support services that UHG is making available.

18. The Wall Street Journal reported that hackers were in Change Healthcare's network for more than a week before deploying ransomware, allowing the hackers to steal significant amounts of data from the company's systems. The cyberattack at Change Healthcare began on February 12, 2024.

- **What day and time did you first learn of the cyberattack? Please be specific.**

Response:

On February 21, 2024, a threat actor deployed ransomware that encrypted numerous systems across the Change Healthcare environment. Responsibility for the attack was claimed by a criminal group known as ALPHV/BlackCat, working with an affiliate. That day, UHG detected the ransomware and took immediate action to mitigate the incident. This included quickly severing connectivity to Change Healthcare's systems to limit the threat of any further contamination by the threat actor.

19. Have you spoken to the Department of Health and Human Services Secretary Becerra about the cyberattack? If so, what day did you first speak with Secretary Becerra? Did the federal government respond timely to the cyberattack?

Response:

Within hours of the ransomware launch, we began cooperating closely with law enforcement, and we continue to work with state and federal agencies to respond to the attack. UHG was in contact with the Department of Health and Human Services (HHS) about this cyberattack no later than February 22, 2024, and our CEO, Andrew Witty, spoke with Secretary Becerra about the incident on March 11, 2024. The company has also been in contact about this incident with federal agencies and other entities including the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Council, the Department of Defense, and the Department of Veterans Affairs. UHG has been in contact with many other government agencies, and this may not reflect a complete list of all the contacts across the company.

20. My understanding is Change Healthcare touches one in three medical records in the United States.

- **How many Americans' protected health information records were accessed by RansomHub? If you don't know the answer to this question, please provide a specific date when you will know.**

Response:

Given the ongoing nature and complexity of the data review, it will take additional analysis before enough information will be available to identify impacted customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

21. Mr. Witty – This cyberattack has caused extensive disruptions not only to critical payments for providers in my state, but also to patients who are eagerly awaiting necessary treatments. The Washington State Hospital Association told me that they have significant concerns about their inability to process prior authorizations for procedures in the wake of this cyberattack. As a result of the cyberattack, many hospitals and health organizations were forced to switch to another system. This switch has caused significant delays in providing care. In many cases where care could not wait, providers have had to deliver it without prior authorization. If the authorization is not granted after the fact, providers are at risk of not being paid at all. All of this is happening while providers are stuck in the prior authorization process that United Healthcare requires them to use. While I appreciate your efforts in getting the system back to normal as soon as possible, you and I both know that patients, especially ones with serious conditions, do not have the luxury of waiting.

Hospitals have continued to provide care for their patients even if they are unable to verify insurance eligibility or get the procedure authorized – because this is the right thing to do, and patients are counting on it. This does not only impact inpatient care. Many people are also having trouble picking up prescriptions, so they are forced to skip refills or pay with cash. As the fourth largest insurance company in the country that owns a pharmacy benefit manager occupying one-quarter of the entire PBM market, United Healthcare has an obligation to ensure that no one falls through the cracks. People's lives are literally at stake.

- **Will you commit to relaxing prior authorization requirements until the system goes back to normal?**
- **How will you ensure that providers who delivered care without prior authorization because they could not obtain it still get paid?**
- **What are you planning to do to ensure that patients receive the procedures and prescription drugs they need in a timely manner?**

Response:

In the aftermath of the cyberattack, UnitedHealthcare temporarily suspended prior authorization for its Medicare Advantage plans, including Dual Special Needs Plans, covering most outpatient services except for Durable Medical Equipment, cosmetic procedures, and Part B step therapies. UnitedHealthcare reinstituted prior authorization on April 15.

In the aftermath of the attack, UHG's priority was to ensure that people had access to the medications and care they needed. For that reason, through Optum Rx, UHG notified network pharmacy partners and pharmacy associations that the Company would reimburse all appropriate pharmacy claims filled with the good faith understanding that the medication would be covered.

For providers, UnitedHealthcare waived or extended deadlines for timely filings and appeals for claim reimbursement that were affected by the Change Healthcare cyberattack; see response to Question 54. In addition to the temporary funding assistance offered to providers at no cost, UHG took these steps in order to support providers and pharmacies and ensure that patients continued to receive the care they needed in a timely manner.

22. Mr. Witty – Since the beginning of the COVID-19 pandemic, hospitals in my state have been facing steep financial losses and workforce shortages due to burnout. Even after the COVID-19 pandemic, providers are still struggling to regain their financial footing. According to the Washington State Hospital Association, hospitals in Washington state lost $3.8 billion during 2022 and 2023. That represents eight straight fiscal quarters of significant losses. This cyberattack on Change Healthcare does not help.

My providers have expressed serious concerns about their inability to receive payments, and they are dealing with a serious lack of communication and clarity from UnitedHealth Group. When I spoke with you in my office, you said that not many providers are using the interest-free loans that United Healthcare offered, implying that the financial situation is not that bad.

However, my providers' financial records paint a different picture. This demonstrates that providers are looking for financial stability and reassurance, not another creditor. Providing health care in the post-pandemic world is already strenuous enough without this disruption. United Healthcare has an obligation to ensure that hospitals can keep their doors open, and that doctors receive their reimbursements in a timely manner.

- **Providers have expressed concern that they will not be reimbursed for procedures provided during the system outage as the prior authorization process United Healthcare mandates was also down. Will you commit to reimbursing providers and relaxing the prior authorization process during this difficult time so that providers have more financial stability?**
- **Will you commit to better communication with providers on the progress of Change Healthcare's system restoration and financial reimbursements?**

Response:

UnitedHealthcare temporarily suspended prior authorizations for Medicare Advantage plans, including Dual Special Needs Plans. The Company also temporarily suspended prior authorizations for most outpatient services except for Durable Medical Equipment, cosmetic procedures, and Part B step therapies. UHC reinstituted prior authorization on April 15. To the extent the Company did not suspend prior authorizations for Medicaid and commercial plans, that is because the decision to do so lies with the plan sponsor (e.g., state governments and corporate customers), not the Company.

The Company has been very active in its efforts to share helpful information about the financial assistance program to providers across the country. This outreach has included the launch of the Change Healthcare Cyber Response website on March 1. This website is frequently updated and has received approximately 650,000 unique visitors and 2.3 million page views. The website also provides information regarding the Company's Temporary Funding Assistance Program, allowing providers to check their eligibility and ask any questions they may have.

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15, approximately $7 billion has been advanced to providers, with 34% of the total funds getting routed to safety net hospitals and federally qualified health centers serving many of the patients and communities at the highest risk. More than 14,000 unique Taxpayer Identification Numbers (TINs) have received funds through the temporary funding program.

In addition, UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance. The Company launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date. UHG prioritized outreach to small community, safety net, and rural providers that are serving the most vulnerable communities and patients.

To access temporary funding assistance, providers need to register and apply by entering their tax identification number. They can then log in to their Optum Pay account to review and accept available funding. Providers will need to apply for funding each week. If the funds are insufficient to meet a given provider's needs or if they need help determining eligibility, they may submit a request through the temporary assistance inquiry form.

Providers have 45 business days to repay any funds UHG advanced. The 45 business day window only opens after the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels. There are no requirements around arbitration, indemnification, or limitation of liability as a condition of accepting funds. Providers can access the program's full terms and conditions by signing into their Optum Pay account.

23. Mr. Witty – Change Healthcare's platforms touch about one in three U.S. patient records. The company processes 15 billion claims per year, totaling more than $1.5 trillion annually. UnitedHealth Group also owns its own pharmacy benefit manager and its own insurer that covers over 49 million people in the US. It also owns Optum, which acquired or hired 20,000 physicians last year.

A company as massive as yours must have top-notch data standards. Protecting patient medical data is essential. And yet I was disturbed to learn that this attack happened through a portal that did not even have multifactor authentication. Multifactor authentication is a basic security measure used by companies and other entities across the country – including here in the Senate.

- **Will you commit to adding a multifactor authentication requirement across Change Healthcare's platforms?**
- **Do you agree that consolidation in the health care industry increases the risk that cyberattackers will be able to gain access to more patient data within one attack?**
- **Do you agree that we need to implement minimum cybersecurity standards for health care companies that receive federal funding?**

Response:

UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally-facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

UHG has seen no evidence that Change Healthcare was attacked because it was part of UHG. Part of the impetus for the acquisition of Change Healthcare was to harness the incredible opportunity presented for everyone in our health care system to innovate, to improve care, to reduce costs, and to reduce burden, but always with our obligations to protect that data top of mind.

Once it acquired Change, UHG began the process of upgrading cybersecurity and information technology, to bring Change Healthcare up to UHG's cybersecurity standards. And in response to this attack, UHG harnessed its substantial resources to respond. These are the resources and the philosophy that underpinned UHG's remediation of health care.gov back in 2013, and its distribution of CMS COVID emergency relief funds to care providers in 2020. UHG's acquisition of Change Healthcare thus helped ensure Change Healthcare was well-

positioned to mitigate the effects of the cyberattack, and, going forward, will serve as the catalyst for improving Change Healthcare's cybersecurity infrastructure and protocols.

UHG supports mandatory minimum cybersecurity standards for the health care industry, including for (1) endpoint protections; (2) remote access, including MFA; and (3) perimeter controls including firewalls. The Company also believes that these minimum standards should be coupled with funding to support small providers in their efforts to meet the standards, which will better protect the entire health care ecosystem.

24. According to the FBI, in 2023 there were 249 ransomware attacks against the health care and public health sector. This was the highest number of ransomware attacks reported by any critical infrastructure sector. These ransomware attacks show no signs of slowing down, which means the healthcare industry must not only be working towards preventing these attacks, but also maintaining cyber resiliency should another attack occur. What I mean by cyber resiliency, is continuing to efficiently provide services and restore business functions after any kind of cyberattack.

- **Before the change healthcare cyberattack, how was UHG working with the federal government, including HHS and CISA, to maintain cyber resiliency should a cyberattack occur?**
- **Based on what you've learned from this attack, what additional tools from the federal government are needed to ensure better resiliency for the next cyberattack?**

Response:

Our security organization receives regular alerts about critical vulnerabilities and other publications about cybersecurity from CISA, the Health Information Sharing and Analysis Center (Health-ISAC), and third-party security providers.

Within hours of the ransomware launch, we began cooperating closely with law enforcement, and we continue to work with state and federal agencies to respond to the attack. UHG was in contact with the Department of Health and Human Services (HHS) about this cyberattack no later than February 22, 2024. The company has also been in contact about this incident with federal agencies and other entities including the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Council, the Department of Defense, and the Department of Veterans Affairs. UHG has been in contact with many other government agencies, and this may not reflect a complete list of all the contacts across the company.

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

25. On April 22nd, UHG confirmed in a press release that "there were 22 screenshots, allegedly from infiltrated files, some containing protected health information (PHI) and personally identifiable information (PII) which could cover a substantial proportion of people in America." I understand UHG paid a ransom to protect this patient data from further disclosure, however, many Texas providers and hospitals remain skeptical and increasingly concerned that this data could still be released now or new data could be compromised in a future attack.

- **Before this cyberattack, were there extra precautions and attention given to protecting millions of Americans' PHI and PII? If so, what was being done by UHG to protect this sensitive data?**
- **What plans are currently in place to protect the sensitive data of providers and patients from a future cyberattack?**

Response:

UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the Company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the Chief Digital and Technology Officer and Chief Information Security Officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

UHG has learned from the attack on Change Healthcare and is strengthening its defenses against cyberattacks in significant ways. The Company has taken a number of steps to ensure that customers and patients feel confident with respect to Change Healthcare's security efforts moving forward, including accelerating efforts to integrate systems to UHG standards; bringing on Mandiant as a permanent advisor to the Audit and Finance Committee of the Board; and committing to sharing our learnings with partners in industry and government, consistent with maintaining applicable privileges.

26. Providers big and small have been hurt by this attack. But I am particularly concerned about the downstream effects for those serving our more vulnerable patient populations, like community health centers. Every single CHC in Texas was affected by this cyberattack because either they or their payors use the Change system for claims reimbursement.

One health center in Texas was facing $14 million in outstanding claims at one point. Another CHC in my state had to eliminate dental services to make ends meet. This could have devastating impacts for the patients these centers serve.

CHCs provide care to uninsured populations and already operate on thin margins. I've heard from health centers across Texas that the solutions and temporary relief options offered by Change were difficult to navigate and ultimately inadequate.

- **Can you please walk us through the financial support options Change offered health centers and other safety-net providers in the face of this attack?**
- **How many providers took advantage of the financial support you were offering?**
- **Did those who passed on these support options give you a reason?**
- **What additional support can be provided to these types of providers who are still struggling financially from the impact of the hack?**

Response:

The Company has been very active in its efforts to share helpful information about the financial assistance program to providers across the country. This outreach has included the launch of the Change Healthcare Cyber Response website on March 1. This website is frequently updated and has received approximately 650,000 unique visitors and 2.3 million page views. The website also provides information regarding the Company's Temporary Funding Assistance Program, allowing providers to check their eligibility and ask any questions they may have.

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15, approximately $7 billion has been advanced to providers, with 34% of the total funds getting routed to safety net hospitals and federally qualified health centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through this temporary funding program.

In addition, UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance. The Company launched a digital campaign to

increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date. UHG prioritized outreach to small community, safety net, and rural providers that are serving the most vulnerable communities and patients.

To access temporary funding assistance, providers need to register and apply by entering their tax identification number. They can then log in to their Optum Pay account to review and accept available funding. Providers will need to apply for funding each week. If the funds are insufficient to meet a given provider's needs or if they need help determining eligibility, they may submit a request through the temporary assistance inquiry form.

Providers have 45 business days to repay any funds UHG advanced. The 45 business day window only opens after the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels. There are no requirements around arbitration, indemnification, or limitation of liability as a condition of accepting funds. Providers can access the program's full terms and conditions by signing into their Optum Pay account.

UHG created the financial assistance program within a week of the attack. The program provided advance payments from the beginning, and UHG never charged any fees, interest, or other associated costs for accessing funds. As UHG learned more information about the circumstances of affected providers and solicited feedback on the program, the Company made changes to its funding program with the aim of helping providers. Based on feedback from providers and government partners in the early launch of the Temporary Funding Program, the Company made several improvements: (1) removed some terms and conditions to simplify the process and expedite payments, (2) extended repayment periods, (3) increased funding amounts, and (4) increased communication/outreach efforts.

The Company's restoration and remediation efforts focused on protecting patients and helping providers, and the Company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

27. Patients and providers are still waiting to hear exactly what protected health information (or PHI) has been implicated in this attack. The HIPAA breach notification rule requires that all covered entities and their business associates notify patients when there is a breach. This was of course an unprecedented attack within the health care industry which could have far-reaching implications across the country for patients and their data privacy.

I have heard from providers who are concerned about the administrative burden that will be required to notify patients, when providers are already stretched thin from this attack. This will be even harder for providers serving harder-to-reach patient populations. Providers are also concerned about how this may negatively affect patient-provider relationships and trust when they themselves were not the ones breached.

- **Is it true UnitedHealth is prepared to take on the responsibility of notifying patients on behalf of providers? What would that process look like exactly for providers?**
- **Should there be changes to this notification policy depending on which covered entities are actually the ones breached?**
- **Should HHS play a bigger role in helping to notify patients?**
- **Are you concerned about how this attack will [a]ffect patients' relationships with providers or UnitedHealth?**

Response:

To help ease reporting obligations on other stakeholders whose data may have been compromised as part of the Change Healthcare cyberattack, UHG has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer where permissible. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

As a Company, we are thankful for the dedication and collaboration that HHS has offered since the early days of our response to this attack. We have met with HHS regularly to provide updates on restoration and to share information so that we could ensure no impacted group was left without support during the disruption.

In terms of changes to the HIPAA breach notification policy and HHS's role in notifying affected patients, UHG stands ready to work with HHS and other governmental stakeholders on efforts to strengthen the health industry's cybersecurity and to streamline notification procedures to help ensure that cyberattack victims and government stakeholders coordinate and avoid duplicative notification efforts.

28. Mr. Witty, as you referenced in your testimony, cyberattacks are becoming more serious and more frequent, despite the best efforts of the Department of Health and Human Services. It will take several months to understand the true scope of this cyberattack and realize how many providers and patients were impacted by this breach. Immediately after the cyberattack was discovered, you took your systems offline.

- **Now that those systems are back up and running, what additional protections or recommendations have been implemented to improve the security of patients and providers' information?**
- **What assurances can you make to health systems across the nation that your network is safe to connect to and UnitedHealth Group is safe to do business with?**

Response:

UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the Company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the Chief Digital and Technology Officer and Chief Information Security Officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

After the February 2024 cyberattack, UHG rebuilt the Change Healthcare systems from the ground up, on an entirely separate network, in order to be certain that the new systems would be clean and safe for use by UHG and its clients. This took significant investment and effort across the UHG enterprise, as returning each service to production required key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, and validation.

Providers and others may request third-party documentation and the company's Assurance Safety Environment Statement via UHG's website.

29. Mr. Witty, United is already the largest employer of physicians in the country, and by all accounts United is continuing to buy physician practices. I am hearing a number of reports from providers that United has taken advantage of the crisis that the Change hack created to justify its purchases and acquire physician practices at a lower cost. As one example, Optum acquired the Corvallis Clinic in Oregon in a fire sale, in part, driven by the group's inability to meet its obligations because of the breach related cash flow interruptions.

- **Can you provide data on how many physician practices you have purchased or made an offer to purchase since the Change healthcare breach?**

Response:

The Company has the highest regard for the Corvallis Clinic in Oregon and is in close communication with the Oregon Health Authority. The Corvallis Clinic acquisition was announced and under review months before the Change Healthcare attack. The price of the transaction has not changed, and the transaction meets all of the regulatory requirements under Oregon law. The Oregon Health Authority viewed the transaction as an opportunity to stabilize and increase a struggling provider's ability to improve patient access and preserve primary care and specialty access in an important area. The Oregon Health Authority determined that there existed an emergency situation that immediately threatened health care services, and that this transaction was urgently needed to protect the interest of consumers.

With respect to other physician practices, neither UHG, nor any of its affiliates, have attempted—or will attempt—to use the cyberattack to develop a strategy for advancing any pending or future acquisitions, which includes a commitment not to use provider information from the temporary relief program to inform our corporate development strategy. This commitment covers the handful of physician practices we have purchased or made an offer to purchase since February 21, 2024.

30. Mr. Witty, United Health has proposed to buy Steward Health Care. Steward has faced serious financial difficulties in recent months impacting many hospitals around the country, including Glenwood Regional Hospital in my state. Deals like this are typically negotiated behind closed doors and have very troubling consequences for competition and consolidation in the health care market.

- **If the United – Steward deal goes through, do you commit to keeping Glenwood Regional and other impacted hospitals open, appropriately staffed, and setting them on a course for financial stability into the future?**

Response:

At the heart of Optum's interest in acquiring Stewardship Health ("Stewardship"), a physician group and subsidiary of Steward Health ("Steward"), is the potential that such a combination provides to grow value-based care models and continue improving health care

delivery to benefit patients. The proposed acquisition does not include Glenwood Regional or any hospitals, which are owned by Steward, not Stewardship.

We understand the future of the Steward-owned hospitals is of paramount concern. We share the concern as the already strained hospital system impacts our current and future patients' ability to receive high quality care. As noted, because the potential combination does not and will not involve acquisition of hospitals, including Glenwood Regional, we defer to Steward for comment on any specific plans it might be considering.

31. Mr. Witty, I have heard from providers that although most of the systems are back online, providers still have reduced access to Electronic Remittance Advice (ERA) data, and limited access to explanation of benefits (EOB) and claim status. This has made it difficult for providers to accurately bill patients for services, and is leading to patients complaining to practices for incorrect billing.

- **When does Change believe that the system will be fully functional in regards to obtaining past ERA and EOBs?**

Response:

UHG continues to make strong progress on restoring services impacted by the event. Indeed, 99% of pre-incident health care systemwide-volumes are flowing smoothly. This is because, in part, the Company found other pathways—through the electrical grid that is our health care system—for many payers and providers to move their claims and payments. With respect to UHG's business, the Company has restored roughly 90% of Change Healthcare's functionality across major platforms and products. The remaining 10% includes products that impact smaller sets of customers and ancillary product features, like eligibility software and analytical tools. The Company expects full restoration of other systems to be completed in the coming weeks.

32. Mr. Witty, as I said to you during the hearing, I have heard directly from several small independent practices in Louisiana which applied for short-term zero-interest loans from United and were denied. Both appealed and eventually received approval, but these were independent practices which could not absorb the cost of not being paid for months at a time.

- **How many providers nationwide applied for loans through United?**
    - **What percentage of those applications have been approved?**
    - **What percentage of those applications had to go to appeal?**
    - **What is the average size loan both in real dollars and as a percentage of amount requested?**
- **What is the average lag time between a provider applying for a loan and actually receiving a check?**

Response:

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15, approximately $7 billion has been advanced to providers, with 34% of the total funds getting routed to safety net hospitals and federally qualified health centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through this temporary funding program, and on average each TIN has accepted over $500,000. The funds are sent by electronic deposit, which takes 2–3 days. UHG has honored nearly every funding request made by a provider experiencing financial hardship.

33. Mr. Witty, you told me during the hearing that United would honor claims from providers who could not obtain prior authorization during the Change outage, even if those claims flowed through Change to other insurance companies.

- **Please provide details of how that claim process will work and how providers seeking payment for claims should proceed.**

Response:

UnitedHealthcare will reimburse claims filed by providers who were not able to obtain prior authorization because of the Change Healthcare outage and who provided care with the good faith understanding that the care would be covered. UnitedHealthcare will not retroactively deny any claims submitted during the pendency of the Change Healthcare outage for services that would have normally required prior authorization. UnitedHealthcare was not in a position to suspend prior authorization for its Medicaid and commercial plans because the decision to do so lies with the plan sponsor, not UHC. Similarly, decisions regarding prior authorization for other health plans lie outside of UHG. Finally, through Optum Rx, UHG also has notified network pharmacy partners and pharmacy associations that we would reimburse all appropriate pharmacy claims filled with the good faith understanding that a medication would be covered.

34. United Health Group (UHG) owns and operates OptumRx, one of the largest pharmacy benefit managers (PBM) – making up 22 percent of the PBM market. In Ohio, numerous independent pharmacy owners have been forced to close their doors, many of whom attribute abusive practices, including the application of direct and indirect renumeration (DIR) fees by PBMs, as a primary reason. In 2023 alone, more than 300 independent pharmacies closed across the country. And as I previously mentioned, which you acknowledged being aware of, over one-third of independent pharmacy owners and managers reported when surveyed that they were considering closing this year due to financial constraints. The Centers for Medicare and Medicaid Services (CMS) issued a final rule that would eliminate the retroactive application of DIR fees beginning in 2024, however these fees are still allowed to be applied at the point-of-sale.

During the hearing, you clarified that – in line with CMS's regulation – OptumRx no longer retroactively applies DIR fees. In fact, you said that your PBM no longer utilizes DIR fees at all.

- **Please clarify: does OptumRx currently apply DIR fees at the point-of-sale, or levy DIR fees at all against pharmacies?**
- **Please list the fees that OptumRx currently collects from pharmacies throughout the transaction process.**
- **Can you confirm that every reimbursement you provide to a pharmacy for filling and dispensing a prescription is sufficient to cover the pharmacy's costs for filling and dispensing the prescription? In other words, does OptumRx ever reimburse a pharmacy below cost for a script filled?**

Response:

The Company complies fully with the recently enacted CMS rule that amended the definition of "negotiated price" to ensure that price concessions are applied uniformly and that the prices available to Part D enrollees at the point of sale are inclusive of all possible pharmacy price concessions. *See* 42 C.F.R. 423 (effective Jan. 1, 2024). In alignment with this regulation, Optum Rx does not retroactively impose DIR fees under Medicare Part D. To clarify further, it is correct that Optum Rx currently does not impose DIR fees at all.

With respect to fees that Optum Rx currently collects from pharmacies, the Company's contracts are the product of individual arms' length negotiations and the terms used to determine compensation, reimbursement, fees, or other consideration vary between contracts.

Similarly, Optum Rx negotiates reimbursement rates with pharmacies for filling prescriptions on an individualized basis. These reimbursement rates vary based on formulary terms and contractual agreement and there is no one-size-fits-all approach. Optum Rx does not have any visibility into each pharmacies total costs for filling and dispensing a prescription. Thus, the Company does not have data to respond to questions about whether reimbursements cover overhead and other associated dispensing costs to pharmacies.

35. Is there a specific timeline UHG has planned on outreach to and providing still-needed financial assistance to smaller providers?

Response:

The Company's outreach efforts have been, and will continue to be, robust. On February 22, the day following the criminal ransomware attack on Change Healthcare's systems, UHG publicly filed an 8-K with the SEC and began communicating regularly with customers about the breach. UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance offered by UHG.

UHG prioritized outreach to small community, safety net, and rural providers that are serving the most vulnerable communities and patients. UHG is providing financial assistance to smaller providers until they can resume regular business operations.

In order to make providers who experienced disruption whole, UHG will continue to ensure that our interest-free, no-fee loan funding capacity remains available for smaller providers until the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels, as our temporary funding assistance program is the best way we can help providers overcome the disruption they have experienced as a result of the cyberattack.

36. Pharmacies and other providers affected by Change Healthcare's shutdown are obligated by HIPAA statute to notify patients when personal health information is compromised. How does United plan to notify providers and pharmacies of what PHI was compromised so these providers can meet their legal reporting obligations?

Response:

To help ease reporting obligations on providers and pharmacies that may have data that was compromised as part of the Change Healthcare cyberattack, UHG has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer where permissible. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

37. Have more advanced cyber security protections been put in place for UHG's many other subsidiaries in light of this attack?

Response:

UHG has learned from the attack on Change Healthcare and is strengthening its defenses against cyberattacks in significant ways. The Company has taken a number of steps to ensure

that customers and patients feel confident with respect to Change Healthcare's security efforts moving forward including accelerating efforts to integrate systems to UHG standards; bringing on Mandiant as a permanent advisor to the Audit and Finance Committee of the Board; and committing to sharing our learnings with partners in industry and government, consistent with maintaining applicable privileges.

38. How will UHG make sure that safety-net providers like Community Health Centers do not continue to face fiscal uncertainty in the aftermath of the Change Healthcare cyberattack?

Response:

The Company has been very active in its efforts to share helpful information about the financial assistance program to providers across the country. This outreach has included the launch of the Change Healthcare Cyber Response website on March 1. This website has been frequently updated and has received approximately 650,000 unique visitors and 2.3 million page views. The website also provides information regarding the Company's Temporary Funding Assistance Program, allowing providers to check their eligibility and ask any questions they may have.

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15, approximately $7 billion has been advanced to providers, with 34% of the total funds getting routed to safety net hospitals and federally qualified health centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through this temporary funding program.

To access temporary funding assistance, providers need to register and apply by entering their tax identification number. They can then log in to their Optum Pay account to review and accept available funding. Providers will need to apply for funding each week. If the funds are insufficient to meet a given provider's needs or if they need help determining eligibility, they may submit a request through the temporary assistance inquiry form.

Providers have 45 business days to repay any funds UHG advanced. The 45 business day window only opens after the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels. There are no requirements around arbitration, indemnification, or limitation of liability, as a condition of accepting funds. Providers can access the program's full terms and conditions by signing into their Optum Pay account.

UHG created the financial assistance program within a week of the attack. The program provided advance payments from the beginning, and UHG never charged any fees, interest, or other associated costs for accessing funds. As UHG learned more information about the

circumstances of affected providers and solicited feedback on the program, the Company made changes to its funding program with the aim of helping providers. Based on feedback from providers and government partners in the early launch of the Temporary Funding Program, the Company made several improvements: (1) removed some terms and conditions to simplify the process and expedite payments, (2) extended repayment periods, (3) increased funding amounts, and (4) increased communication/outreach efforts.

The Company's restoration and remediation efforts focused on protecting patients and helping providers, and the Company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

In addition, UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance. The Company launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date. UHG prioritized outreach to small community, safety net, and rural providers that are serving the most vulnerable communities and patients

39. How do UHG and Optum plan to protect independent pharmacies in this particularly difficult time by working with them, not just the big chains, to make sure claims operations are set up and reimbursement is fair?

Response:

Pharmacy support was the first area of focus when restoring systems, as the Company wanted to ensure that people had access to the medications they needed. Through Optum Rx, UHG notified network pharmacy partners and pharmacy associations that we would reimburse all appropriate pharmacy claims filled with the good faith understanding that a medication would be covered. And for patients who could not use their coupons during the Change Healthcare outage, the Company has been and will continue to contact those patients and honor their coupons to ensure that the patients are reimbursed for their out-of-pocket medication expense they incurred and thus made whole.

UHG is committed to working with small and independent pharmacies to ensure their claim operations are fully restored and back online. As of late April, pharmacy claims services had returned to 99.8% of pharmacies. The small number of remaining pharmacies all either have restoration plans in progress or outreach has occurred.

UHG regularly updates the public about product restoration efforts on its dedicated cyber response website, which may be found at http://www.uhg.com/changehealthcarecyberresponse. Our website lists all impacted systems, date of restoration or anticipated restoration, and the current status (uninterrupted/fully restored, partial service available, restoration in progress, and restoration date pending).

40. During the midst of Change's systems being down, did United decrease the number of claims that required prior authorization in order to decrease burdens on providers and patients, as CMS recommended?

- **If so, what difference did it make?**
- **Will United consider removing prior authorization requirements for some services permanently as a lesson learned?**

Response:

In the aftermath of the Change Healthcare cyberattack, UnitedHealthcare temporarily suspended prior authorization for its Medicare Advantage plans, including Dual Special Needs Plans, covering most outpatient services except for Durable Medical Equipment, cosmetic procedures, and Part B step therapies. By taking these proactive temporary steps, UHG sought to ensure providers could continue to deliver patients the access to care and medications that they needed.

UHG is committed to working with government and industry stakeholders to modernize the health care system, including the prior authorization system. We are actively exploring new ways to address the challenges prior authorization is trying to address—namely, patient safety and minimizing waste in the system. Even prior to the Change Healthcare cyberattack, the Company launched an effort to reduce our prior authorization codes across the Company's business lines. We are committed to continuing to innovate and improve the timeliness and efficiency of our business to maximize patients' access to appropriate, evidence-based care.

41. Please explain your experience working with the FBI.

- **How could they have helped you solve problems faster or have been more proactive?**

Response:

Within hours of the ransomware launch, we contacted the FBI, and we remain in regular communication. We shared critical information, including details about the intrusion, the method of attack, Indicators of Compromise, 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.

42. As I mentioned during the hearing, there are significant risks when health care and financial information are breached. For older adults – whose victimization from scams have skyrocketed in recent years – a data breach means even more of their information is available to scammers to use against them in the future.

- **In addition to credit monitoring, how is UnitedHealth Group (UHG) assisting older adults whose data may have been captured in the breach? In particular, what advice or assistance is the company offering related to breached health data?**

Response:

In addition to free credit monitoring and identity theft protections for two years, UHG has also created a dedicated call center staffed by clinicians to provide support services. Any individual concerned that their data has been impacted should visit www.changecybersupport.com or call 1-866-262-5342 to find more details regarding the support services that UHG is making available.

The company, along with leading external industry experts, continues to monitor the internet and dark web to determine if data has been published. There were 22 screenshots, allegedly from exfiltrated files, some containing PHI and PII, posted for about a week on the dark web by a malicious threat actor. No further publication of PHI or PII has occurred at this time. To date, the Company has not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.

43. You've noted that UHG is doing everything possible to minimize the possibility of personal health information being leaked.

- **What specific activities is the company undertaking in pursuit of that goal? How is the company preventing further exploitation of protected health information (PHI) by bad actors?**

Response:

UHG is continuing to cooperate with law enforcement during the ongoing investigation. Minimizing the possibility of the exploitation of PHI remains highly important. UHG is actively undertaking many actions to this effect, including engaging with Mandiant as a permanent advisor to the Audit and Finance Committee of the Board, working with leading external industry experts to monitor the web for signs of data disclosure, and offering free credit monitoring and identity theft protections to anyone impacted.

44. You also mentioned that UHG is offering free credit monitoring and identity theft protections for two years. However, once this data is out in the world, it has lasting implications. This is especially true for children's data whose been stolen. As I mentioned, this data can be a blank slate for cyber criminals to open up bank accounts and apply for loans, and often takes years for people to realize this has occurred.

- **What long term services does UHG plan to provide to ensure patients health information, especially that of children, are not used against them in the years to come?**

Response:

Please see our response to your Question 42.

45. During the hearing, you addressed the majority of Finance member's concerns as United's "top priority." I appreciate your willingness to engage as quickly as possible to resolve the challenges and security concerns for patients and providers alike. However, I would appreciate more clarity on what you mean by "top priority."

- **Can you please elaborate on the concrete actions you are taking for each of the following, what their order of prioritization will be, and the timeline for each?**
  - **The implementation of multi-factor authentication across systems.**
  - **Identifying patients harmed by the data breach.**
  - **Identifying types of data breached.**
  - **Ensuring providers have adequate cash flow or have received loans.**

Response:

UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally-facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

Based on initial targeted data sampling to date, the Company has found files containing protected health information ("PHI") or personally identifiable information ("PII"). Given the ongoing nature and complexity of the data review, the Company expects that it will take additional analysis before enough information will be available to identify affected customers

and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

UHG obtained a dataset that is safe for the Company to access and analyze from the FBI weeks after the ransomware attack, so it took some time to be in a position to analyze the affected data. Further, this analytical process has to be done very methodically, and it requires a significant amount of time and compute resources to unpack and unzip all of the relevant files. UHG is following gold standard processes utilized by companies seeking to make reasonable and broad notifications, which take time. The Company is working as quickly as it can, consistent with these standards, but does not yet have a specific date by when it expects the analysis will be complete.

Rather than waiting to complete the data review, UHG is providing free credit monitoring and identity theft protections for two years, along with a dedicated call center staffed by clinicians to provide support services. Any individual concerned that their data has been impacted should visit www.changecybersupport.com or call 1-866-262-5342 to find more details regarding the support services that UHG is making available.

UHG created the Temporary Funding Assistance Program for providers within a week of severing connectivity to the affected Change Healthcare systems. The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. And as of May 15, approximately $7 billion has been advanced in the form of (1) accelerated payments UHG made and (2) no cost, no-fee loans. Indeed, around 34% of these loans have gone to safety net hospitals and federally qualified health centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through the Company's Temporary Funding Program.

For the loans provided under the program, UHG provides funds to any provider that is experiencing a shortfall in cash flow as a result of the outage in the Change Healthcare systems. UHG initially calculated the loan amounts by attempting to predict the amount of cash a provider may need, but its efforts to do so were based on incomplete information, given that UHG does not have visibility of all funds flowing to any provider from across the entire health care system. UHG therefore allowed providers to tell it how much money they required to meet shortfalls when they applied for loans. UHG then approved the amounts. For requests under a million dollars, UHG deposited funds into the providers' Optum-based accounts within hours. For larger requests, UHG's underwriters typically approved the amount within days.

46. How is UHG/Change Healthcare testing its rebuilt IT environment to ensure it is clear of vulnerabilities and safe to use following the cyberattack? When does the company expect it will be safe to resume use of the IT infrastructure?

Response:

UHG rebuilt the Change Healthcare systems from the ground up, on an entirely separate network, in order to be certain that the new systems would be clean and safe for use by UHG and its clients.

In a matter of weeks, UHG replaced thousands of Change Healthcare laptops, rotated credentials, rebuilt the data center network and core services, and added new server capacity. UHG effectively built a brand-new functioning data center and workforce. In addition, UHG reissued around 11,000 clean devices to Change Healthcare employees and contractors, which were delivered globally over a two-week period. At the same time, UHG was able to use Optum's back-up system to help some providers carry on without interruption. UHG also rerouted some clients to competitors after the incident and is now encouraging clients to have at least two alternative channels in case of any future interruptions. After this initial rebuild, the Company quickly began relaunching services, with each product undergoing key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, validation, and more.

Providers and others may request third-party documentation and the company's Assurance Safety Environment Statement via UHG's website.

47. You committed to delaying loan repayment deadlines until the backlog of claims have been cleared, regardless of timeframe. You also noted that this would be determined by providers themselves.

- **What concrete steps is UHG taking to communicate these flexibilities to providers? What will be the process for providers to determine their own timelines for repayment?**

Response:

UHG launched www.uhg.com/changehealthcarecyberresponse on March 1, which has been frequently updated and has up-to-date information about the Company's temporary funding assistance program. In addition, the Company also launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date.

While we continue to make progress in mitigating the impacts of the cyber-attack on Change Healthcare services, we understand that some providers are still affected as certain systems come back online. Our top priority has been to continue to provide the support providers need for as long as it takes to get their claims and payments flowing at pre-incident levels. We actively worked through the individual nature of the recovery. To provide continued financial assistance, we have two targeted waves of emails, new banner language alerting our flexibility to providers on our Temporary Funding Assistance Program ("TFAP") landing page and our cyber response website. In addition, we have also reached out to have one on one verbal conversations

with providers to ensure they are aware that we are not creating a one-sized fits all date for repayment.

We have taken a personalized approach to determining providers' funding requests and restoration efforts. In those one-on-one verbal conversations with providers we are communicating that we will work with them on a case-by-case basis so they can determine when their business is back to normal. We have no intention of asking for repayment until providers determine their business is back to normal. Once providers determine their business is back to normal we will work with each provider to determine when the 45 business days will start with no fees or interest.

For additional information about the temporary funding process and applicable deadlines for providers' repayments, we encourage providers to complete an inquiry form on our website or call 1-877-702-3253.

48. You have stated multiple times that Change was a newly acquired system by UHG. You also noted that Change was already up and running when UHG acquired it, meaning there was no period of time in which Change did not interact with patient and provider data.

- **What, if any, procedures do UHG have in place to ensure adequate cybersecurity for newly acquired systems, especially for those in a position to interact with providers and patient data?**

Response:

After an acquisition, UHG takes steps to apply UHG standards to the newly-acquired entity's information technology and cybersecurity infrastructure. The same is true with Change Healthcare. Change Healthcare was a 40-year-old company with networks, products, and systems built on top of one another over the last 40 years. Addressing that layered infrastructure takes time. Following the close of the acquisition in October 2022, UHG began working to bring the legacy infrastructure Change Healthcare had in place in line with UHG's standards.

UHG's Security Shield program is one method by which UHG works to improve the cybersecurity posture of newly acquired entities. Security Shield is a set of high-priority controls and best practices that UHG deploys to new acquisitions to bring them to a baseline level of security.

49. During the hearing, you mentioned that as of May 1, UHG now has multi-factor authentication on all external services.

- **Can you clarify what this means, how you will verify these external systems are properly using multi-factor authentication, and what steps you are taking for internal systems?**

Response:

UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the Company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the Chief Digital and Technology Officer and Chief Information Security Officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally-facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

50. As a result of the cyberattack and its fallout, many providers went through the onerous task of switching clearinghouses, which is a costly and time-consuming process.

- **Does UHG intend to reimburse providers for any charges, outside of those for patient care, they incurred due to the attack?**

Response:

The Company's restoration and remediation efforts focused on protecting patients and helping providers, and the Company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or

are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

To the extent providers have incurred other costs associated with the attack, UHG is committed to reviewing their issues and working to resolve their concerns on a case-by-case basis.

51. During the hearing, multiple Senators asked questions about Optum's provider network. You noted that UHG has 10,000 physicians and contracts with an additional 80,000.

- **How many of these physicians, contract or otherwise, currently practice in Pennsylvania?**

Response:

Optum's practices in Pennsylvania employs or contracts with approximately 100 physicians (data current as of June 2024).

52. "Due to the Change Healthcare cyberattack, I have heard from Rhode Islanders who have suffered due to the lack of redundancy and preparation by UnitedHealth Group (UHG). I've heard from a patient who experienced a 10-day delay getting their prescription filled and from a Providence mental health provider who did not receive a single payment from UHG's Optum insurer for over two months, leading them to miss payments on their mortgage and car. The financial strain nearly forced them to close their small practice. UHG, through Optum, established a temporary assistance program to extend short-term loans to affected health providers and organizations, yet our providers in Rhode Island still faced potential practice closures.

- **What system redundancies does UHG plan to implement so patients and providers are not left without medications and payments in the future?"**

Response:

To mitigate service disruptions, UHG offered Change Healthcare customers Optum alternatives for several key product areas including data analytics, risk coding, risk adjustment, claims submission, and compliance reporting. One example includes directing Change Healthcare claims clearinghouse customers to use Optum Intelligent Electronic Data Interchange (iEDI), a claims submission tool for providers. The iEDI claims submission portal allows a range of providers, from large health systems to independent family practices, to submit claims for reimbursement. Additionally, to support pharmacies impacted by disruption to Change Healthcare services such as MedRX, UHG rolled out the Optum Rx Pharmacy Portal. This portal assists pharmacies in the Optum Rx network with everyday tasks including claims status and

history, and patient eligibility. UHG has also committed to reimbursing pharmacies for all pharmacy claims filled with the good faith understanding that a medication would be covered. For patients who could not use their coupons during the Change Healthcare outage, the Company has been and will continue to contact those patients and honor their coupons to ensure that the patients are reimbursed for their out-of-pocket medication expense they incurred and thus made whole. UHG also rerouted some clients to competitors after the incident and is now encouraging clients to have at least two alternative channels in case of any future interruptions.

53. "UHG is the nation's largest private health insurer and the largest employer of physicians. It ranks as the nation's fourth-largest company by revenue this year, with nearly 5 percent of gross domestic product flowing through UHG's systems each day. UHG's subsidiary, Change Healthcare, processes 40 percent of the nation's medical claims. The February cyberattack froze payments, preventing hospitals and providers from being paid for weeks. With much of America's health system running through a single organization, thousands of hospitals and doctors are vulnerable to a single point of failure.

- **Has the size of UHG in the US economy made it a particular vulnerability to our health care system?"**

Response:

UHG's size and sophistication can make our health care system less vulnerable to attack. Change Healthcare had aging infrastructure and legacy systems. At the time of the attack, we were in the process of upgrading cybersecurity and information technology, to bring Change Healthcare up to UHG's cybersecurity standards. Part of the impetus for the acquisition was to harness the incredible opportunity presented to our health care system to innovate, to improve care, to reduce costs, and to reduce burden, but always with our obligations to protect individuals' data top of mind. In response to this attack, we harnessed the substantial resources of UHG to respond.

We believe that our business model is helping to accelerate the transition from volume to value; moving beyond a transaction-based health system to a model that is designed to be proactive to help keep people healthy over the course of a lifetime. One that rewards high-quality care, delivers better outcomes, and drives lower costs.

The U.S. health system remains deeply fragmented and rooted in fee-for-service models that put the burden of finding and navigating care squarely on the shoulders of the people who need help the most. The resulting lack of coordination too often results in less-than-optimal patient outcomes, higher mortality rates, poor patient experience, redundant care, and waste. UHG's integrated ecosystem enhances coordination and the quality of patient care.

54. At the Finance Committee hearing on May 1st, Mr. Witty verbally committed to extending timely filing deadlines for UnitedHealthcare plans for any claims and appeals impacted by the Change Healthcare cyber hack and subsequent system outage.

- **Please confirm in writing that UnitedHealthcare is committed to waiving or extending timely filing requirements for all affected providers utilizing Change Healthcare. Please specify which dates of service for claims and remittance dates will be included in UnitedHealth's waived or extended timely filing deadlines.**
- **What is the specific extension, in terms of calendar days from the date of service, that UnitedHealth will provide for claims submission?**
- **What are the specific extensions, in terms of calendar days from the original remittance date, that UnitedHealth will provide for claim resubmission, correction, and reconsideration?**

Response:

UnitedHealthcare waived timely filing requirements for all providers impacted by the Change Healthcare incident for any claims received starting February 15, 2024, for many UnitedHealthcare fully insured commercial, UnitedHealthcare Medicare Advantage, UnitedHealthcare community plans and UnitedHealthcare Individual Exchange plans, also referred to as UnitedHealthcare Individual & Family ACA Marketplace plans. Notably, for Medicaid plans, individual states determined the timely filing deadlines for their respective UnitedHealthcare community plans. The waiver does not apply to self-funded commercial plans administered by UnitedHealthcare. Although overall claims flow into UnitedHealthcare returned to normal levels in mid-March, UHC kept these waivers of filing deadlines in place to provide additional relief to the system.

Now that provider claims are flowing again, the company intends to resume timely filing requirements on June 15. We will continue to proactively accommodate providers who have remained with Change Healthcare but have not returned to pre-incident claim submission volumes by ensuring that timely filing deadlines remain waived for those particular providers. UnitedHealthcare will also make clear to providers that they may contact their UnitedHealthcare relationship manager or a Provider Services help desk for additional support as needed.

55. The Change cyberattack has resulted in a significant administrative burden for providers.

- **How does UnitedHealth Group plan to adequately compensate these providers for the incurred costs, particularly additional labor, that were essential to preserving their ability to deliver essential health services during the system outage?**

Response:

The Company's restoration and remediation efforts focused on protecting patients and helping providers, and the Company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero cost, zero interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

To the extent providers have incurred other costs associated with the attack, UHG is committed to reviewing their issues and working to resolve their concerns on a case-by-case basis.

56. In light of the Change service outage, what specific actions are being taken to facilitate the Indian Health Service's (IHS) recovery process? Additionally, how does UnitedHealth Group plan to ensure that Tribes are actively engaged and included in your assistance programs to alleviate the impacts of this outage?

Response:

The Change Healthcare team responsible for managing IHS accounts engaged with IHS and provided temporary workarounds during the outage periods. We were in regular contact with the cyber security lead for IHS, providing regular updates, and also spoke directly with the IHS Chief Information Security Officer (CISO) as part of CHC's nationwide outreach to federal agency CISOs. As with the rest of CHC's clients, services have been largely restored to CHC's IHS clients, with a small number of exceptions of IHS clients for whom we continue to work to restore connectivity. IHS clients have also received funding through the Temporary Funding Assistance Program.

57.

58. Will UnitedHealth Group commit to providing notifications and offering credit monitoring services for all IHS patients affected by the Change outage?

Response:

UHG is committed to providing reasonable and broad notice to IHS individuals whose data was affected by the Change Healthcare cyberattack. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

Like any other individual concerned that they might be impacted, IHS patients are eligible for free credit monitoring and identity theft protections for two years. Any IHS patient can visit changecybersupport.com or call 1-866-262-5342 to find more details regarding the support services that UHG is making available.

59. Please provide a detailed timeline outlining when IHS can expect to receive precise information regarding the impact on patients and the extent of data compromised in the Change breach.

Response:

UHG is committed to providing appropriate notice to affected individuals, including IHS patients. To help ease reporting obligations on other stakeholders whose data may have been compromised as part of the Change Healthcare cyberattack, UHG has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer where permissible. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

UHG is working as quickly as possible to develop a complete and accurate assessment of the individuals impacted by this cyberattack. Given the ongoing nature and complexity of the Company's data review, the Company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

59. Reports indicate that the Change hackers demanded a ransom payment of $22 million worth of Bitcoin —please confirm whether or not this was the case, and whether UHG was given any other options of payment platforms for the ransom payment.

Response:

UHG paid the demanded $22 million ransom in bitcoin. Because this is an active law enforcement investigation, we will not provide further comment. Additional questions should be directed to the involved law enforcement agencies, including the FBI.

60. Did UHG make this payment? If so:

- **Have you been informed whether law enforcement able to track the ransom payment along the Bitcoin blockchain?**
- **If so, what was the ultimate disposition of this payment?**

Response:

Please see our response to your Question 59.

61. UHG is the largest corporate employer of physicians in the country, potentially in violation of certain state Corporate Practice of Medicine (CPOM) laws. Passed in the 19th century, these laws were intended to insulate health care providers from outside forces that might seek to influence their clinical decision-making, prohibiting non-physicians, or lay entities, from owning provider practices. But today, state CPOM laws are largely unenforced and marred with loopholes, leaving provider practices vulnerable to corporate takeover. For example, to circumvent state CPOM laws, private equity firms and insurers, including UnitedHealth's provider subsidiary Optum, form management services organizations (MSOs) that contract with a physician practice to manage its billing and administration. Although the practice's clinical operations remain nominally owned by a licensed physician, the practice is often completely managed and operated by the MSO. As a result, providers are often forced to put corporate profits over the interests of their patients.

- **What percentage of UHG's affiliated physicians work in physician practices that use UHG's MSO services?**
- **What are the common terms of the UHG physician agreements –**
  - **What percentage of physician contracts include non-competes**
  - **What percentage include, stock transfer restriction agreements,**
  - **What percentage include non-disclosure or other gag clauses?**
  - **What percentage include other provisions to restrict physicians' autonomy and control over the practice?**
- **Do the use of these terms differ between directly employed vs. MSO affiliated physicians?**

Response:

Optum is proud to partner with independent, affiliated physicians. Optum employs roughly 9,000 physicians. Optum does not employ any contracted or affiliated physicians. These affiliated physicians contract with Optum's risk-bearing, independent practice association (IPA) entities, who in turn contract with health plans under a value-based risk contract. These affiliated physicians are independent of Optum, and Optum does not provide management services to any physician practices within Optum's IPA networks, except in the limited circumstances where the independent physician practices need assistance to manage risk contracts. Where we do provide affiliated physicians with MSO support, in order to assist them in managing risk contracts, these agreements are limited to providing claims administration, financial reporting, technology, and related support. Less than three percent of affiliated physicians receive MSO support from an Optum MSO. Optum holds no investment or ownership interest in such independent practices.

Optum's model is to support physicians in a manner to allow them to focus on the patient, remove administrative burdens, and assist physicians with tools to help them move from fee-for-service to value-based care. As it pertains to Optum's physician employment agreements, Optum does not use a single physician employment agreement form in every state that it operates. Rather, the physician employment agreements often are unique to each Optum practice and comply with each state's unique law.

Physician employees of the Optum practices have access to a host of confidential, proprietary, and trade secret information related to the practice, and Optum requires physician employees to maintain the confidentiality of confidential, proprietary, and trade secret information. The confidentiality provisions in employment agreements do not prevent a patient from receiving their medical records under state law in the event their physician moves to another employer.

Further, our physician employment agreements do not include stock transfer restrictions. Our employment agreements do not restrict a physician's autonomy or control over their practice of medicine.

62. Along with a bevy of vertically-integrated subsidiaries, UHG employs or is affiliated with over 90,000 doctors -- about one in every 10 doctors in the country. And while you clarified in your testimony that UHG only directly employs roughly 10,000 out of those 90,000 doctors, you have never disclosed how exactly the other 80,000 doctors are classified. Instead, in the hearing, you merely claimed that "they choose to work with [UHG]," without providing any details of their contracts.

- **What percentage of employed or affiliated physicians contract only with UHG?**
- **What percentage of employed or affiliated physicians have non-compete agreements? Please break down this percentage by physicians who are directly employed and those that are employed by an MSO affiliate.**
- **What percentage of directly employed physicians are required to take coding training courses? What percentage of affiliated doctors have risk-coding incentives in their contracts?**
- **How does Optum structure ownership and affiliation of physician practices? To what extent does it use a management services organization (MSO) to employ physicians directly?**
- **Are UnitedHealth insurance sales agents involved with Optum practices? If so, what are their roles and responsibilities? Do these roles and responsibilities include switching patients' coverage to UnitedHealth?**
- **How is UHG's ownership or affiliation of Atrius Health and Reliant Medical Group in Massachusetts structured?**

Response:

Optum is proud to partner with independent, affiliated physicians. Optum employs roughly 9,000 physicians. Optum does not employ any contracted or affiliated physicians. These affiliated physicians contract with Optum's risk-bearing, independent physician association entities, who in turn contract with health plans under a value-based risk contract. These affiliated physicians are independent of Optum.

As the "affiliated physicians" are independent physician practices, Optum does not control with whom those practices contract. Affiliated physicians may also contract with other IPAs and contract directly with health plans. The contracts between Optum and the affiliated physicians are network participation agreements. None of the network participation agreements include non-competes.

Optum physician practices are multi-payer, meaning that they affiliate with other payers in addition to UnitedHealthcare. Our physician practices see patients that are covered by state, federal, and commercial health care plans. Optum's physician practices, as well as its independent practice associations that contract with Medicare Advantage plans, comply with CMS's Medicare Marketing Guidelines. UnitedHealthcare insurance sales agents are not involved in the management, operation, or business of Optum physician practices.

Optum provides training to all its employed physicians, including training on the MA risk adjustment model, diagnosing, documentation, and coding, among other topics in accordance with federal regulatory and coding accreditation guidance. Optum performs annual reviews of employed and affiliated physician incentives and does not approve risk-coding incentives.

Optum owns the management service organizations that provide the full-scope of administrative, management, and support services to the Atrius Health and Reliant Medical Group physicians practices. The structure of Optum's ownership and management related to Atrius Health and Reliant Medical Group is identical, consistent with Massachusetts' law, and were both submitted for review and approval by Massachusetts' Health Policy Commission and the Office of the Attorney General. As was disclosed to the HPC, both the Atrius and Reliant physicians retain their clinical practice autonomy and the arrangement with Optum supports the growth and expansion of each of the practice's unique care model, which delivers value to the patient through the provision of high-quality care at lower total medical expense.

Please also see responses to Questions 31 and 61.

63. Leveraging its vertically integrated structure, UHG can effectively keep much of its business in-house, sending payments from its insurance arm to its various provider subsidiaries. For example, in 2023 alone, Optum received 62 percent of its total revenue from UHG's insurance arm. More broadly, UHG sent $138 billion – 25 percent of its revenue – to its own subsidiaries in 2023.

- **Has UHG ever been the subject of a transfer price-related audit by federal regulators?**
- **A 2023 Wall Street Journal investigation revealed that UHG was significantly marking up drug prices at its vertically integrated specialty pharmacies, potentially in an effort to skirt federal regulations capping insurer's profits. Does UHG send higher payments to its provider subsidiaries, including OptumRx, than independent providers?**

Response:

The WSJ article misrepresents important information, and we disagree in strong terms with the picture it paints. It is unclear to us how the calculations in the article were performed and how the highlighted drugs were chosen as a sample. The article also misunderstands some important fundamentals of the pharmaceutical supply chain. For example, the premise of the article is wrong: UnitedHealth Group does not set prices of any drugs or "mark up" drug prices; drug manufacturers set drug prices and Optum Rx (the Pharmacy Benefit Manager) reimburses pharmacies for the drugs they dispense according to the reimbursement terms in pharmacy network contracts negotiated with those pharmacies. Optum Rx uses the same reimbursement approach for affiliated pharmacies as it does for comparable independent pharmacies. The article also incorrectly states that "PBMs decide which medicines a patient's health plan will pay for and how much the patient will have to contribute to the cost, in the form of out-of-pocket expenses like deductibles and coinsurance." That is wrong; payers control plan design and make those decisions. And, as the company stated at the time the article was published, patients would pay less out-of-pocket using UnitedHealth insurance plans than they would buying 15 out of 20 drugs examined by the article through the Cuban pharmacy, and none of the drugs are frequently used by UHC's patient population. Our insurance business is subject to regular oversight and review by various state and federal regulatory authorities to ensure that pricing is in compliance with applicable regulatory requirements.

64. UHG is the largest private insurer in Medicare Advantage (MA), and federal regulators have found that your company has engaged in aggressive upcoding of MA enrollees – that is, making patients appear sicker than they actually are to secure higher payments from the federal government. Alarmingly, UHG's direct control of physicians indeed helps facilitate this gaming in MA, as UHG can pressure doctors and other health care professionals to add extra diagnosis codes to their patients' medical charts.

- **To what extent does UnitedHealth use chart reviews, health risk assessments, or other data analytic techniques to capture diagnoses for risk-adjusted payments under Medicare Advantage and value-based payment models?**
- **Does UnitedHealth require physicians to attend HCC coding trainings? Are physicians subject to discipline if they do not attend? Does UnitedHealth preference UHC patients when scheduling annual wellness visits?**
- **Does UnitedHealth establish goals or bonuses for physicians or other employees related to the use of chart reviews, health risk assessments, or other data analytic techniques to capture diagnoses for risk-adjusted payments under Medicare Advantage and value-based payment models?**

Response:

We strongly disagree with the suggestion that UHG was found to engage in upcoding. Our value-based care payment models use chart reviews and health risk assessment to identify where members might have health care related gaps in care and to validate when those gaps in care have been addressed. UHG does not set bonuses based on the use of chart reviews, health risk assessments or other data analytic techniques for value-based payment models, although such information may be consulted when determining if quality targets have been achieved.

Optum provides training to all its employed physicians, including training on the MA risk adjustment model, diagnosing, documentation, and coding, among other topics in accordance with federal regulatory and coding accreditation guidance.