United States Senate

WASHINGTON, DC 20510

April 29, 2024

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20598

Dear Director Easterly:

We are writing regarding the ongoing ransomware attacks against UnitedHealth Group (UHG) subsidiary Change Healthcare (Change) that are driving physicians to bankruptcy, interrupting essential care services like pain management for cancer patients, and leaking sensitive patient data—causing massive disruptions to the nation's health care system.[1] Nearly two months after the initial attack, a second ransomware gang has taken control of the stolen data and begun leaking patient records on the dark web, threatening to sell the entire trove to the highest bidder unless UHG pays another multi-million-dollar ransom.[2] Given the urgency of this threat, Congress must have a full accounting of the cybersecurity landscape including the events leading up to, and after, the Change cyberattack.

On February 21, 2024, Russian-linked cybercriminal group ALPHV Blackcat conducted a ransomware attack on Change, the largest processor of medical claims in the United States.[3] This attack, in which the cybercriminal group shut down Change platforms until it received a $22 million Bitcoin ransom payment, caused widespread and ongoing disruptions to the nation's healthcare system.[4] Seven weeks later, on April 8, 2024, a second ransomware group, RansomHub, took control of the stolen data and is demanding additional payment. And RansomHub has begun leaking sensitive patient data to up the ante.[5] These attacks highlight a dire need for stronger tools to crack down on ransomware attacks.

[1] AMA, "Change Healthcare cyberattack impact," 2024, https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf; Tech Crunch, "Change Healthcare stolen patient data leaked by ransomware gang," Zach Whittaker, April 15, 2024, https://techcrunch.com/2024/04/15/change-healthcare-stolen-patient-data-ransomhub-leak/.

[2] Tech Crunch, "Change Healthcare stolen patient data leaked by ransomware gang," Zach Whittaker, April 15, 2024, https://techcrunch.com/2024/04/15/change-healthcare-stolen-patient-data-ransomhub-leak/.

[3] Wired, "Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment, Andy Greenberg, March 4, 2024, https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/; The Washington Post, "Health-care hack spreads pain across hospitals and doctors nationwide," Daniel Gilbert, Dan Diamond, Christopher Rowland, and Kim Bellware, March 3, 2024, https://www.washingtonpost.com/business/2024/03/03/change-health-care-hack-hospitals/.

[4] Wired, "Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment, Andy Greenberg, March 4, 2024, https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/.

[5] Wired, "Change Healthcare Faces Another Ransomware Threat—and It Looks Credible," Matt Burgess, April 12, 2024, https://www.wired.com/story/change-healthcare-ransomhub-threat/.

Following the February ransomware attack, Change disconnected more than 100 of its technology platforms which impacted thousands of patients and providers.[6] For example, UHG estimated that more than 90 percent of 70,000 pharmacies in the U.S. had to change how they process electronic claims, creating a severe cash squeeze.[7] Across the country, pharmacies have been barred from filling prescriptions, doctors are forced to wait on prior authorization, medical centers cannot pay their employees, and tens of millions of dollars in insurance payments to providers are delayed.[8] Indeed, according to a group representing 5,000 U.S. hospitals, health systems, and other health care organizations, the February attack was "the most significant cyberattack on the U.S. healthcare system in American history."[9]

The ramifications of the Change attack will have prolonged effects on our health care system.[10] This month, the American Medical Association (AMA) released survey findings that "practices will close because of this incident, and patients will lose access to their physicians. The one-two punch of compounding Medicare cuts and inability to process claims as a result of this attack is devastating to physician practices that are already struggling to keep their doors open."[11] Providers are growing increasingly desperate, facing a massive cash crunch that, in some cases, threatens their ability to remain in business.[12]

Now, in a shocking turn of events, a second cybercriminal group, RansomHub, posted to the dark web that it "has 4 terabytes of Change Healthcare's stolen data, which it threatened to sell to the 'highest bidder' if Change Healthcare didn't pay an unspecified ransom."[13] RansomHub recently published a small subset of data on the dark web and is threatening to post more,[14] marking the first time in these string of attacks that cybercriminals have actually leaked stolen information as evidence that they

[6] Wall Street Journal, "Medical Providers Fight to Survive After Change Healthcare Hack," James Runle, Catherine Stupp, and Kim S. Nash, March 1, 2024, https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a.

[7] NPR, Health care company ties Russian-linked cybercriminals to prescriptions breach, Jenna McLaughlin, March 1, 2024, https://www.npr.org/2024/03/01/1235255804/pharmacies-ransomware-prescriptions-unitedhealth; New York Times, "Cyberattack Paralyzes the Largest U.S. Health Care Payment System," Reed Abelson and Julie Creswell, March 5, 2024, https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

[8] *Id*.

[9] American Hospital Association, "AHA Urges Congress to Provide Support to Help Minimize Further Fallout from Change Healthcare Attack," March 4, 2024, https://www.aha.org/lettercomment/2024-03-04-aha-urges-congress-provide-support-help-minimize-further-fallout-change-healthcare-attack.

[10] Stat News, "Change Healthcare cyberattack outage could persist for weeks, UnitedHealth Group executive suggests," Brittany Trang, February 29, 2024, https://www.statnews.com/2024/02/29/change-healthcare-cyber-attack-outage-will-last-for-weeks/; New York Times, "With Cyberattack Fix Weeks Away, Health Providers Slam United, Reed Abelson and Julie Creswell," March 8, 2024, https://www.nytimes.com/2024/03/08/health/united-healthcare-cyberattack.html.

[11] AMA, "Physicians struggle to keep practices afloat after Change cyberattack," press release, April 10, 2024, https://www.ama-assn.org/press-center/press-releases/physicians-struggle-keep-practices-afloat-after-change-cyberattack.

[12] New York Times; Stat News, "Change Healthcare cyberattack outage could persist for weeks, UnitedHealth Group executive suggests," Brittany Trang, February 29, 2024, https://www.statnews.com/2024/02/29/change-healthcare-cyber-attack-outage-will-last-for-weeks/; The American Prospect, "UnitedHealth Exploits an 'Emergency' It Created," Maureen Tkacik, March 10, 2024, https://prospect.org/health/2024-03-10-unitedhealth-exploits-emergency-change-ransomware-oregon/.

[13] Wired, "Change Healthcare Faces Another Ransomware Threat—and It Looks Credible," Matt Burgess, April 12, 2024, https://www.wired.com/story/change-healthcare-ransomhub-threat/.

[14] Cyber News, "Ransomware gang publishes part of stolen Change Healthcare records," April 16, 2024, Gintaras Radauskas, https://cybernews.com/news/ransomware-gang-ransomhub-change-healthcare/.

have medical records in their possession.[15] The leaked information represents a portion of millions of patients' sensitive and personal data, including insurance records, billing files, and medical information.[16]

Unfortunately, this attack is emblematic of a growing trend in which cybercriminal groups gain access to, and install ransomware on, a computer system, encrypt the system's data, and require a ransom payment in order to decrypt the files. If the victim does not pay the ransom, attackers either increase the ransom amount, or destroy the decryption key–making it possible for the victim to regain access to the system.[17]

In 2022, ransomware attacks impacted at least 2,421 local governments, schools, and healthcare providers in the U.S.[18] According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."[19] Despite government intervention in 2021, attacks on schools nearly doubled from 1,043 in 2021 to 1,981 in 2022, and attacks on local governments increased over 30 percent, including one incident in Miller County, Arizona, where a compromised mainframe spread malware to endpoints in 55 different counties.[20] According to the Department of Health and Human Services, there were over 460 ransomware attacks affecting the U.S. health care and public health sector.[21] These numbers do not account for underreporting: the FBI notes that reporting of malware attacks is "artificially low."[22] Most of these attackers are located abroad. In 2021, nearly 75 percent of all ransomware revenue went to Russia-linked entities.[23]

According to a 2022 report by the Senate Committee on Homeland Security and Government Affairs (HSGAC), ransomware payments are almost exclusively made using cryptocurrency, typically Bitcoin, due to the payment method's decentralized, anonymized, and irreversible nature.[24] In the case of Change, blockchain analysts observed that on March 1, ten days after this years' ransomware attack, "a Bitcoin address connected to ALPHV Blackcat received 350 bitcoins in a single transaction, or close to

[15] Tech Crunch, "Change Healthcare stolen patient data leaked by ransomware gang," Zach Whittaker, April 15, 2024, https://techcrunch.com/2024/04/15/change-healthcare-stolen-patient-data-ransomhub-leak/.

[16] *Id*.

[17] Wired, "Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment, Andy Greenberg, March 4, 2024, https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/.

[18] Emsisoft Software Lab, "The State of Ransomware in the US: Report and Statistics 2022," January 2, 2023, https://www.emsisoft.com/en/blog/43258/the-state-of-ransomware-in-the-us-report-and-statistics-2022/.

[19] World Economic Forum, "The Global Risks Report 2022," January 11, 2022, p. 9, https://www.weforum.org/publications/global-risks-report-2022/.

[20] Emsisoft Software Lab, "The State of Ransomware in the US: Report and Statistics 2022," January 2, 2023, https://www.emsisoft.com/en/blog/43258/the-state-of-ransomware-in-the-us-report-and-statistics-2022/.

[21] Department of Health and Human Services, "Ransomware & Healthcare," p. 18, https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf.

[22] United States Senate Committee on Homeland Security and Government Affairs (HSGAC), "Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns," March 22, 2022, p.38, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf.

[23] Chainalysis, "Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity," February 14, 2022, https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/.

[24] *Id*., p. 3.

$22 million based on exchange rates at the time."[25] These funds are at high risk of being laundered through the crypto ecosystem – including via centralized crypto exchanges and crypto mixers, the "preferred methods for laundering ransomware payments"[26] – complicating law enforcement's ability to recover the ransom.

As the nation's cyber defense agency and coordinator for critical infrastructure security, the Cybersecurity and Infrastructure Security Agency (CISA) leads the nation in understanding and responding to cyberattacks against critical American infrastructure, and its StopRansomware.gov website is one of the few places that ransomware attacks are reported.[27] The latest attacks on Change Healthcare underscore the urgent need for more oversight and investigation into the frequency, scope, and root causes of these attacks, specifically with regards to cryptocurrency's role.

The people hurt by these ransomware attacks have a right to know what the federal government is doing to protect them. We urge you to provide responses to our questions below that are publicly releasable to the maximum extent possible. Classification should not be a basis for failing to provide responsive information, as our office is able to receive and handle classified information accordingly and upon request. With this in mind, we ask that you answer the following questions, on a question-by-question basis, by May 13, 2024:

1. How many reports of ransomware attacks has CISA received for each year between 2018 and the present?
    a. What is the total value of the reported ransomware payments during this time period?
    b. What percentage of payments were made using cryptocurrency?
2. What percentage of ransomware attacks does CISA believe are unreported?
3. In your assessment, how big is the threat of ransomware attacks in the United States?
    a. To what extent are these threats exacerbated by the use of cryptocurrency?
4. What steps has CISA taken to estimate the scope of ransomware attacks and address the dangers from them?
    a. Has CISA estimated the total cost of ransomware attacks on the U.S. economy, including costs arising from computer system repairs and productivity losses? If so, please detail these figures.
5. Can CISA provide information on the number of thwarted healthcare-related ransomware attacks?
    a. How were these attacks intercepted?
6. How can CISA better prepare the healthcare industry for increasing ransomware attacks and ensure the sector can maintain access to patient care and access to life-saving services in the event of a ransomware attack?
7. Has CISA estimated the potential costs of ransomware attacks on the healthcare industry?
8. How is CISA cooperating with the Department of Justice (DOJ), Federal Bureau of Investigations (FBI), and other federal agencies to track and combat ransomware attacks?
9. In March 2023, CISA announced the establishment of the Ransomware Vulnerability Warning Pilot (RVWP) to "determine vulnerabilities commonly associated with known ransomware

[25] Wired, "Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment, Andy Greenberg, March 4, 2024, https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/.

[26] Chainalysis, "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," February 7, 2024, https://www.chainalysis.com/blog/ransomware-2024/.

[27] Cybersecurity and Infrastructure Security Agency (CISA), "About CISA," https://www.cisa.gov/about.

exploitation and warn critical infrastructure entities with those vulnerabilities, enabling mitigation before a ransomware incident occurs."[28]

   a. What is the status of the RVWP?
   b. Please describe the results of the pilot and if there are any plans to extend or renew it.

10. Given that virtually all ransomware attacks rely on payments made through cryptocurrency, what additional actions can legislators, regulators, and law enforcement officials take to address cryptocurrency's unique threats?

    a. How does CISA usually approach these problems?
    b. How frequently does CISA recover any ransom?
    c. Do victims ever get money back?
    d. Do individuals get credit monitoring?
    e. What is required of hospitals or other public entities after they are attacked? Do they get fined for data that is leaked?
    f. Do physicians and small clinics get any relief for lost monies?
    g. Is there something like a customer care center for victims of ransomware attacks?

11. Can you share your rapid response plans? Do you have any contingency scenario planning and how often do you update it?
12. What efforts has CISA made to ensure individuals are incorporating resiliency procedures and processes specifically for industries in critical infrastructure to ensure operation post attack?

CISA'S Efforts Specific to the Change Healthcare Attack

13. When was CISA alerted to the Change attack? By whom?
14. What role is CISA playing in responding to the Change attack?
    a. How is it collaborating with its interagency partners including the FBI and DOJ?
    b. How is it collaborating with UHG?
15. What information did CISA share with UHG regarding ALPHV Blackcat and its ransom methods? When?
16. What information does CISA typically share with health care entities, including UHG, regarding cyber threats? To whom does CISA typically share this information with in these organizations?

Sincerely,

Elizabeth Warren
Elizabeth Warren
United States Senator

Bill Cassidy, M.D.
Bill Cassidy, M.D.
United States Senator

[28] CISA, "CISA Establishes Ransomware Vulnerability Warning Pilot Program," press release, March 13, 2023, https://www.cisa.gov/news-events/news/cisa-establishes-ransomware-vulnerability-warning-pilot-program.

Richard Blumenthal

Richard Blumenthal
United States Senator