DATA BREACH AT THE D.C. HEALTH EXCHANGE

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

AND THE

SUBCOMMITTEE ON OVERSIGHT

OF THE

COMMITTEE ON HOUSE ADMINISTRATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

APRIL 19, 2023

Serial No. 118–23

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
51–895 PDF WASHINGTON : 2023

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
SHONTEL BROWN, Ohio
JIMMY GOMEZ, California
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
BECCA BALINT, Vermont
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Senior Policy Analyst
PETER WARREN, Senior Advisor
MALLORY COGAR, Deputy Director of Operations and Chief Clerk
CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

GERALD E. CONNOLLY, Virginia, *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida

COMMITTEE ON HOUSE ADMINISTRATION

BRYAN STEIL, Wisconsin, Chairman

BARRY LOUDERMILK, Georgia
H. MORGAN GRIFFITH, Virginia
GREG MURPHY, North Carolina
STEPHANIE BICE, Oklahoma
MIKE CAREY, Ohio
ANTHONY D'ESPOSITO, New York
LAUREL LEE, Florida

JOSEPH MORELLE, New York, *Ranking Member*
TERRI SEWELL, Alabama
NORMA TORRES, California
DEREK KILMER, Washington

TIM MONAHAN, Staff Director
CONTACT NUMBER: 202-225-8281

JAMIE FLEET, Minority Staff Director & Chief of Staff
CONTACT NUMBER: 202-225-2061

SUBCOMMITTEE ON OVERSIGHT

BARRY LOUDERMILK, Georgia, Chairman

H. MORGAN GRIFFITH, Virginia
GREG MURPHY, North Carolina
ANTHONY D'ESPOSITO, New York

NORMA TORRES, California, *Ranking Member*
DEREK KILMER, Washington

C O N T E N T S

WITNESSES

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

DATA BREACH AT THE D.C. HEALTH EXCHANGE

Wednesday, April 19, 2023

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
JOINTLY, WITH THE
COMMITTEE ON HOUSE ADMINISTRATION
SUBCOMMITTEE ON OVERSIGHT
Washington, D.C.

The Subcommittees met, pursuant to notice, at 3:03 p.m., in room 2154 Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee on Cybersecurity, Information Technology, and Government Innovation] presiding.

Present from the Committee on Oversight and Accountability [Subcommittee on Cybersecurity, Information Technology, and Government Innovation]: Representatives Mace, Timmons, Burchett, Edwards, and Connolly.

Present from Committee on House Administration [Subcommittee on Oversight]: Representatives Loudermilk, Steil, Griffith, Torres, and Morelle.

Also present: Representative Norton.

Ms. MACE. All right, my partner in crime, the gentleman from Virginia, has arrived, so we are going to get started.

Mr. CONNOLLY. Now that we know what time we are supposed to start.

Ms. MACE. Yes. Thank you, Mr. Connolly. So, the Subcommittee on Cybersecurity, Information Technology, and Government Innovation and the Subcommittee on Oversight will come to order.

I would like to begin by welcoming Mr. Connolly—good afternoon, sir—as we tiptoe in, but also by welcoming House Administration Oversight Subcommittee Chairman, Barry Loudermilk, and Ranking Member Norma Torres. We also have with us Chairman Bryan Steil and Ranking Member Joe Morelle. We are pleased for you all to join us today. After conferring with Chairman Loudermilk, we agreed that today's joint hearing will operate under the rules of the Committee on Oversight and Accountability.

Without objection, Congresswoman Eleanor Holmes Norton of Washington, DC. is waived on to the Subcommittee this afternoon for the purpose of questioning witnesses.

Without objection, the Chair may declare a recess at any time.

I now recognize myself for the purpose of making an opening statement.

First of all, good afternoon and welcome. This is a joint hearing of this panel, the Subcommittee on Cybersecurity, Information Technology, Government Innovation in the House Oversight and Accountability Committee, and the House Administration Committee's Subcommittee on Oversight, which is chaired by the gentleman from Georgia to my left, Mr. Loudermilk. Since this is a joint hearing, we will all have opening statements from the Chair and Ranking Member of both Subcommittees. That is a total of four opening statements, so I am going to keep my remarks as brief as possible.

First, I want to explain why we are conducting this hearing jointly. The data breach we are going to get to the bottom of today is of great concern to Members of Congress, staff, Federal employees, and all those who use the D.C. Health Exchange. The overwhelming majority, about 90 percent, of the Exchange enrollees are not affiliated with Congress. So this is not just about us, this is about everybody who has been affected by this breach.

There are people who get health insurance through the Exchange as individuals or employees of one of over 5,000 participating small businesses. This data breach is the latest in a troubling string of cyber breaches exposing confidential data of ordinary Americans. All too often these breaches involve government agencies or programs to whom people are entrusting their most personal information.

We know the recent data breach at D.C. Health Benefit Exchange Authority resulted in the theft, sale, and public posting of confidential personal information of thousands of individuals getting health insurance via the Exchange, and that may not be the fullest extent of the breach. Indeed, the vulnerability through which the breach occurred may have actually exposed up to 200,000 or more individuals to hackers and exposed their personal information.

Last month, several internal health insurance enrollment reports maintained by D.C. Health Link were accessed without authorization and then posted online. These Excel spreadsheets sold and posted on the dark web contain data including the personal information on each Exchange enrollee listed. That would be their name, their date of birth, their age, their Social Security Number, telephone numbers, their home addresses, mailing addresses, email addresses, their employer, their health plan, their health insurance premium, race, ethnicity, citizenship status, and more.

The advent of AI is only going to make breaches like this even more vulnerable to personal data, and it will only get worse if businesses and government agencies are ill-prepared for what lies ahead. People should be able to sign up for healthcare without surrendering to public view their most confidential personal information. So, the Subcommittees are convening here today to find out, with the help of our witnesses, how this data breach happened, and I do expect to have some concrete, substantive answers because if we filibuster here today, none of us are going to be happy. This is too important to not get the information.

We want to know who is responsible. We are going to want an answer for that. And we are going to want to know how those responsible are going to be held accountable. Do they even still have a job today? It would be one of my first questions. And what is being done to ensure that this does not ever happen again?

And with that, I would like to yield to the Ranking Member of this Subcommittee, Mr. Connolly from Virginia.

Mr. CONNOLLY. Thank you so much, Madam Chairwoman, and thank you for convening this hearing, and very much enjoy collaborating with our colleagues today.

In 2022, Federal Bureau of Investigation's Internet Crime Complaint Center received over 800,944 phishing, personal data breach, or other complaints, representing estimated losses of more than $10.2 billion, an increase of more than $3.3 billion from just the previous year. As we stated during our last Subcommittee hearing, data breaches, including government data breaches, are no longer unusual incidents.

In 2015, an OPM data breach, for example, exposed the private information of nearly 22 million American individuals, including my own personal information. 2019, the Russian Foreign Intelligence Service compromised SolarWinds software, which is widely used across the Federal Government. And in 2021, Microsoft reported that China's Ministry of State Security exploited vulnerabilities in their Exchange service.

Today we are here to talk about the recent D.C. Health Link data breach, which affected 56,415 individuals, including 17 Members of Congress, 43 of their family members, and 585 House staff members and 231 of their family members. Despite D.C. Health Link's robust cybersecurity practices, including the use of leading commercial cybersecurity solutions, next-generation firewall protections, and increased stress testing efforts, the organization remained vulnerable to attack.

According to the investigative findings to date, an undetected human error caused this breach. It was not underlying IT technical issues, legacy IT systems, or even understaffing, a human error left the data base vulnerable to unauthorized access. A breach demonstrates that even organizations with sophisticated cybersecurity practices must remain vigilant to potential risks because one small oversight is the only window an opportunistic hacker needs to break in.

The breach also demonstrates that bad actors may not only hide in the dark web. They may also, as in recent high-profile cases, use stolen data that landed easily on accessible public websites where the bad actor published the information to gain notoriety. Our cybersecurity posture must adapt to this new ecosystem. Fortunately, law enforcement has been working aggressively to dismantle key players in the cybercrime echo system, including those associated with this very breach we are considering today.

On March 15, the FBI took down the website *BreachForums*, the online hub of illicit activity used to expose the D.C. Health Link data, and arrested its alleged founder. While I acknowledge the D.C. Health Benefit Exchange Authority's commitment to protecting the data of customers from another breach, the fact of the matter is that the information of more than 56,000 people has been

compromised, putting their physical safety and financial security at some risk. These individuals join hundreds of millions of Americans who have had their data stolen in the past year alone, and data breaches are only going to grow in scope.

We need to move swiftly to implement the national cyber strategy examined in this Subcommittee just last month, which will drive important changes to better-protect Americans' sensitive data. Throughout my career in the private sector, and local and Federal Governments, I have championed a trifecta cybersecurity strategy that encompasses modernizing IT systems, building a skilled Federal cybersecurity workforce, and, most importantly perhaps, fostering a security-centric culture at all levels of government.

One of the primary ways Congress can enforce the trifecta is through consistent and sustained oversight of Agency compliance with the Federal Information Technology Acquisition Reform Act, which grew out of this Committee, FITARA. Through the scorecard we have and the hearings we have on that scorecard, and I very much appreciate Chairwoman Mace recommitting this Subcommittee holding those updated hearings, we have promoted effective IT modernization by empowering Agency CAOs and ensuring they have a seat and a voice in decision-making. We are proud of the scorecard that has secured big victories for the IT community by elevating CAOs within their agencies to ensure they are key players in fundamental conversations.

In today's hearing, we need to hear a strategy from D.C. Health Benefit Exchange Authority to improve oversight and internal governance proceedings. They must continue to act urgently to address remaining cybersecurity concerns, provide resources to breach victims, and instill the safeguards needed to prevent future breaches.

I agree with Chairwoman Mace. We want to hear answers today, not excuses, so that we can try to make sure that this sort of thing does not happen again, and that we protect the privacy of those who have had their data breached. With that I yield back. Thank you, Madam Chairwoman.

Ms. MACE. Thank you. I now recognize Chairman Barry Loudermilk for the purpose of making an opening statement.

Mr. LOUDERMILK. Well, thank you, Chair Mace, for partnering with our Subcommittee to hold this joint hearing, and for hosting us in your Committee room here today.

On March 6, data was breached from the D.C. Health Exchange and posted on the dark web. As a result, the personal identifiable information of tens of thousands of people was exposed. This includes over 800 Members of Congress, their staff, and families who are required by law to use D.C. Health Link. The fact that such a breach was able to occur left our congressional community in shock.

It is well-known that the U.S. Congress is a key target for cyberattacks, both foreign and domestic. That is why the Chief Administrative Officer has an Office of Cybersecurity that sets high standards for vendors and contractors hoping to do business with the House. These safeguards help protect Members, staff, and their families' data from thousands of cyberattacks that happen every

month. Unfortunately, the D.C. Health Link is not subject to those same standards.

Now, prior to serving in Congress, I spent 30 years in the information systems industry, both in the public and private sector, so I know just how vital it is to ensure that there are high standards and protocols in place when dealing with personal identifiable information.

Our goal for today's hearing is two-fold. First, we must learn how this breach was able to happen and how we can minimize the harm to all individuals impacted. Second, we must discuss the improvements that those who support the House need to make to ensure that those impacted by this breach are never put in this position again. Also, I would like to discuss the preliminary findings from the forensic report produced by Mandiant, a well-known cybersecurity firm that was hired by the D.C. Health Exchange in the aftermath of the breach. That 7-page report was shared with us on Friday, and while we are hoping it would provide more clarity, we were left scratching our heads.

We still do not know who is behind the attack. We still do not know if the data is for sale on other areas of the dark web. We still do not know how much data the hacker accessed, and we still do not know exactly how this was able to occur. However, the report largely blames Amazon Web Services, when, interestingly enough, Mandiant is a subsidiary of Google, one of AWS' largest competitors. While we invited representatives from Mandiant to come and testify today and answer some of our questions, they declined. That is disappointing.

This breach occurred at a time when threats to Members of Congress are still at historic highs. I know this firsthand. It is unacceptable that over a month later, we still do not have answers and continue to be left in the dark. I look forward to getting answers and learning what steps we can take to better-protect this information. Thank you, and I yield back.

Ms. MACE. Thank you. I would now like to recognize Ranking Member Norma Torres for the purpose of making her opening statement.

Mrs. TORRES. Thank you to the Chair, and I want to join my colleagues in welcoming Ms. Szpindor and Ms. Kofman. Thanks for coming before our Committee today.

The recent data breach to the D.C. Health Benefit Exchange compromised the personally identifiable information, including the names, birth dates, and Social Security numbers of more than 56,000 individuals, jeopardizing their privacy and financial security. And as Members and congressional staff seeking employer-sponsored health insurance were required to enroll in the marketplace as created by the Affordable Care Act back in 2014, the affected universe of the data breach also included a significant number of individuals here on Capitol Hill. I understand those affected individuals include 17 Members of Congress, 435 House staff, and more than 270 spouses and dependents.

A significant breach like this one further demonstrates the importance of ensuring that all organizations have the necessary cybersecurity tools to combat cybercrime. Most recently, in my own home region of the Inland Empire, I learned about how hackers at-

tacked a local 911 Center. This is a reminder that all systems are fragile and at risk of hacking threats. Today's hearing provides us with an opportunity to examine how the D.C. Health Benefit Exchange and other similar organizations can better-protect against potential cybersecurity risks and work to ensure that this will never happen again.

Ms. Kofman, I was pleased to hear in your testimony that D.C. Health Link is undergoing a comprehensive security review and assessment of your entire system, and I look forward to hearing more about what you have learned so far. And I urge you to continue to work through any remaining cybersecurity vulnerabilities, including those susceptible to both malicious activity and simple human error.

Ms. Szpindor, in the days after the breach, you clarified to Members in the Committee on House Administration the breach did not include any House systems, and stated that the portal used by the House to communicate with the D.C. Exchange was well-protected, and as you mentioned in your testimony, the House is often a target of cyberattacks. And I look forward to hearing more about how our administrative professionals at CAO continue to work to protect the House from cyber threats, ensuring that we have the necessary protections in place to avoid further breaches.

Finally, I would like to thank the CAO, the Capitol Police, the House Sergeant at Arms, and the FBI for their work on this matter in the days and weeks after the data breach. And with that, I yield back to the Chair.

Ms. MACE. Thank you. I am pleased to introduce our witnesses for today's hearing. Our first witness is Ms. Mila Kofman, the Executive Director of the D.C. Health Benefit Exchange Authority, or HBX, the D.C. Exchange. HBX is a public-private partnership established to develop and operate the online health insurance marketplace called D.C. Health Link for residents and small businesses in the district. Our second witness is Ms. Catherine Szpindor, the Chief Administrative Officer of the U.S. House of Representatives. Ms. Szpindor is responsible for Member and staff services, including information technology and additional business functions. We welcome everyone and pleased to have you this afternoon.

Pursuant to Committee Rule 9(g), the witnesses will please stand and raise your right hands.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[A chorus of ayes.]

Ms. MACE. Let the record show that the witnesses all answered in the affirmative.

We appreciate both of you being here today and look forward to your testimony. I would like to remind the witnesses that we have read your written testimony and it will be entered and will appear in full in the record. Please limit your oral arguments this afternoon to 5 minutes to give us time before votes today to ask our questions.

As a reminder, please press the button on the microphone in front of you when you are speaking so that it is on, and Members can hear you. When you begin to speak, the light in front of you

will turn green. After 4 minutes, the light will turn yellow. When the red light comes up, your 5 minutes has expired and we would ask that you please wrap up your statements.

I recognize Ms. Kofman to please begin her opening statement.

STATEMENT OF MILA KOFMAN
EXECUTIVE DIRECTOR
D.C. HEALTH BENEFIT EXCHANGE AUTHORITY

Ms. KOFMAN. Thank you. Good afternoon, and thank you for inviting me today. My name is Mila Kofman. I am the Executive Director of the D.C. Health Benefit Exchange Authority, and I want to say how sorry I am. I know this is personal for many of you, many of your colleagues and many staff members. We failed to prevent the theft of two reports which had sensitive personal information of our customers. I want you to know that we have not and will not fail in our response, and we are working hard to make sure this never happens again.

I am here to discuss the D.C. Health Link data breach affecting 56,415 current and past customers, including Members of Congress, their families and staff. On March 6, 2023, we learned that a threat actor stole personal data from D.C. Health Link. While we do not have medical or healthcare information, we do have personal sensitive information. The two stolen reports had personal information like name, date of birth, and Social Security Numbers.

On day one, March 6, we immediately asked the FBI Cybersecurity Task Force for help and had two special agents in our offices that afternoon. We also engaged a leading cybersecurity firm, Mandiant. On day two, law enforcement obtained and shared the two stolen reports with us. By day three of the breach, Mandiant identified the source of the breach, and my staff shut it down immediately. By day four, we secured 3 years of identity theft and credit monitoring protection for all three major credit bureaus for our affected customers and notified them on March 9 as soon as Experian provided us with a toll-free number and generated codes for our customers to use to sign up.

Although there was no evidence that additional data was stolen outside of the two stolen reports, out of abundance of caution, we offered the same 3 years of identity theft and credit monitoring protection services to other customers. We provided public updates on March 8, 10, and 14, and also set up a dedicated web page on *dchealthlink.com*. We briefed three U.S. House Committees. We also briefed the D.C. business community and others we work with.

On Friday, April 14, Mandiant completed its report. The cause of this breach is a server that was misconfigured which allowed access to the two stolen reports without proper authentication. The investigation shows the misconfiguration was not intentional. To be clear, it was a human mistake. At no point was the D.C. Health Link enrollment system breached. We have a strong cybersecurity program, which includes technologies used by U.S. intelligence agencies and Fortune 100 companies, and have successfully repelled attacks on our network.

In response to the breach, I immediately asked third-party cybersecurity experts to conduct a comprehensive review and assessment of our entire environment, including a sweep to ensure there was

no other malicious activity within it, and a review of our cloud environment, our code, our configurations and our processes and procedures. We are now focused on a comprehensive review and making improvements. We are also actively investigating how the misconfiguration occurred. I can update you when we know more.

I want to reiterate how deeply sorry we are that two reports were stolen with personal information. We are making every effort to ensure this does not happen again. Thank you for inviting me to speak today, and I look forward to answering your questions.

Ms. MACE. Thank you. I now recognize Ms. Szpindor to begin her opening statement.

STATEMENT OF CATHERINE L. SZPINDOR
CHIEF ADMINISTRATIVE OFFICER
U.S. HOUSE OF REPRESENTATIVES

Ms. SZPINDOR. Thank you, Chairwoman Mace, Chairman Loudermilk, and Ranking Members Torres and Connolly, and other Members of the House Oversight and Accountability Subcommittee on Cybersecurity Information Technology, and Government Innovation, and the Committee on House Administration Subcommittee on Oversight.

The House's information-sharing relationship with D.C. Health Link dates to 2013 when Members and staff first enrolled in the D.C. Health Link healthcare programs for calendar year 2014. The CAO's relationship with the D.C. Health Link is compulsory in nature and is limited to the secure exchange of information required to facilitate House participation in its healthcare programs as required by the Patient Protection and Affordable Care Act, effective January 1, 2014, and the subsequent Office of Personal Management rulings pertaining to the law's implementation.

Each month, D.C. Health Link and the CAO follow established secure data transfer protocol to pay healthcare premiums, report terminations, and fix information discrepancies. All the Federal and state entities that the CAO shares Member and staff data with, including the D.C. Health Benefit Exchange Authority, are required to comply with Federal and state security requirements as well as their own. Once data is received by another entity, the CAO's jurisdiction ends. The CAO lacks the authority and capacity to validate or mandate the security measures employed by other government entities it is required to interface with.

Upon learning about the D.C. Health Link breach late morning Tuesday, March 7, 2023, the CAO's cyber team confirmed none of the servers nor applications supported by the House has been compromised. The CAO worked with the House leadership between March 7 and March 10 to send a series of communications first to the potential universe of impacted individuals then to the confirmed universe of impacted individuals providing information on freezing their and their family's credit at the three major credit bureaus out of abundance of caution. They also received steps individuals should take to avoid becoming a victim of financial fraud. Notices were sent to impacted individuals no longer employed by the House, but whose information was confirmed to have been included in the breach. Additionally, the CAO participated in separate brief-

ings for Members and staff and included important breach updates in payroll and benefits newsletters distributed House-wide.

The CAO Payroll and Benefits team continues to field calls from the House community pertaining to the breach. Everyone in the House community, past and present, ever considered eligible for healthcare via D.C. Health Link is eligible for 3 years of free credit and identity monitoring services paid for by D.C. Health Link.

This incident, like the 2015 OPM breach, is a sobering reminder of why cybersecurity is our top priority. Each year the CAO deploys over a quarter million software patches, protects more than 3,000 servers and stops tens of millions of attempted cyberattacks and billions of attempted probes. We have continuously improved our cybersecurity posture. With the support of House leadership, we address staffing deficiencies and significantly increased behind-the-scenes improvements and capabilities to include enhanced real-time network monitoring, better malware detection tools, and improved security controls over devices and applications.

A strong cybersecurity posture requires consistent strict adherence to security practices and training by every member of the House community. The House is a target. We must remain vigilant and have the right policies and capabilities to ensure we protect House data and are prepared to quickly address security issues, should they arise.

The CAO appreciates the opportunity to testify today, and we look forward to working with you and the other legislative branch partners as the D.C. Health Link investigation continues.

Ms. MACE. Thank you. Thank you, both. I would now like to recognize myself for 5 minutes for questioning.

You said, Ms. Kofman, earlier that the breach was due to a misconfigured server without proper authentication. So, is this sort of like an exposed IP address? Is this a password issue with authentication on the server? What actually happened?

Ms. KOFMAN. What we know based on Mandiant's findings and investigation is that we had a misconfigured server.

Ms. MACE. What does that mean?

Ms. KOFMAN. If you had an IP address, you can access the server without proper authentication.

Ms. MACE. So, it was an exposed IP address that——

Ms. KOFMAN. If you had the IP address, you can access the information on the server.

Ms. MACE. And how long was the server misconfigured? I guess how long was the IP address exposed?

Ms. KOFMAN. So, we are still investigating. The initial configuration of the server, we know occurred mid–2018.

Ms. MACE. So, the server IP address was exposed starting in 2018?

Ms. KOFMAN. The initial configuration of the server was mid–2018. Right now, we have external——

Ms. MACE. Was that the same IP address for that server when this was exposed as in 2018? Is it the same? Was it the same IP address? Had it changed at all in that timeframe? From the time it was configured, to the time that the breach—did it have the same IP address that entire time?

Ms. KOFMAN. I do not know if it had the same IP address. I will have to get back to you. But right now, we have external experts I have asked to investigate the actual misconfiguration, what happened, when it happened, why it happened, who was involved, how it happened. We have external investigators taking a look. Once I have more information——

Ms. MACE. Is the individual or the team of individuals that set up the servers in 2018, and, well, we do not know when it was misconfigured. Are those individuals still employed or still a vendor of D.C. Health Link, the individuals or the team of people that set up the server?

Ms. KOFMAN. So, that is why we are doing an external investigation to identify who was involved in setting up all of the configurations, all of the settings when that server was being integrated with Slack, and our suspicion is that it happened over time. And, so, our external investigators are looking into, starting 2018, what happened. And they are going to be looking at every year that that server was configured to identify.

Ms. MACE. So, it is possible the exposure had happened over an extensive period of time since 2018, potentially?

Ms. KOFMAN. Part of that time that server was down. So, we are in fact-finding mission right now, and I——

Ms. MACE. How long was the server down during that timeframe?

Ms. KOFMAN. I do not know. Meaning offline? So, our——

Ms. MACE. How do you not know when the server was down? That seems like if you knew it was down, you would know the timeframe it was down.

Ms. KOFMAN. That is why we have external investigators taking a look to see when it was actually online, when it was offline, so we can document everything and identify who was involved, how it was configured.

Ms. MACE. Was it an employee or was it a contractor?

Ms. KOFMAN. We have employees and we have contractors, and so that is part of our ongoing investigation being conducted by external experts. And I am happy to provide you with all of that information when we have it.

Ms. MACE. So, given that we do not know the timeframe, and the server was set up in 2018, is it possible that more than 56,000 people were exposed, like hundreds of thousands of people's data was exposed? Is that a possibility?

Ms. KOFMAN. So, what we know is 56,415 people, their information was stolen. We know that for a fact. We know that another set of consumers, current and past customers, their information was stored in the same manner that the stolen reports were stored. We have no evidence that their information was stolen.

Ms. MACE. So, on this server were there are only two reports? Or the two reports that were exposed were the only ones you are aware of? Or was there more than two reports on the server?

Ms. KOFMAN. The server had multiple reports, and the server had other automation jobs. Some of the reports we know did not have any personal information. Other reports had personal information, and that is why——

Ms. MACE. Up to how many people could potentially have been exposed in from this breach?

Ms. KOFMAN. We are investigating that, but that is why we notified pretty much everyone.

Ms. MACE. I mean, but certainly you know by the number of reports on that server, the reports that have personal data and do not, certainly you know the number of records or number of people that were exposed to the breach?

Ms. KOFMAN. The issue is some reports existed for a week, and then were replaced by the report, so they were eliminated. We are trying to identify every potential person whose data may have been on the server, and that is why we notified a lot of people whose——

Ms. MACE. Yes. No, I get that, and I am not going to complain about the way that people were notified. I think that was done well. I would tell you it was done quickly, it was done well and, from a crisis standpoint, the response was excellent.

Ms. KOFMAN. Thank you.

Ms. MACE. I am more concerned about the access to the IP address, the exposed IP address and the data that was on that server. Just as a company policy within the D.C. Health Exchange, are employees required to use a "strong password" when they are creating, you know, authentication within the programs that that you all use?

Ms. KOFMAN. Yes. We encourage the use of strong passwords for——

Ms. MACE. Is it required or is it just encouraged?

Ms. KOFMAN. We follow D.C. government standards for our passwords.

Ms. MACE. Do you all require as a matter of company policy two-factor authentication for company passwords that are used by employees or contractors?

Ms. KOFMAN. I will have to get back to you on what contractors are required to do.

Ms. MACE. What about employees? Are they required to use two-factor authentication for their passwords for anything that they are accessing within the organization?

Ms. KOFMAN. Yes, it might be helpful to give you——

Ms. MACE. Are they required to use two-factor authentication? "Yes" or "no."

Ms. KOFMAN. Multi-factor authentication is required to access your systems, like your cellphone, your email if——

Ms. MACE. How long has that been going on?

Ms. KOFMAN. The multi-factor authentication requirements? I will double-check. I think for a number of years now.

Ms. MACE. OK.

Ms. KOFMAN. And before you had to have codes to get in, but I will double-check that.

Ms. MACE. So, because we do not know who is responsible for it yet. No one has been held accountable. No one has been fired or lost a contract as a result of the breach. Would that be accurate to say?

Ms. KOFMAN. We are doing a full investigation——

Ms. MACE. Are you going to fire the contractor or the employee that created this breach issue? Will they be fired?

Ms. KOFMAN. We are doing a full investigation.

Ms. MACE. That would be a "no" or "I don't know," which is not an acceptable answer. I have one question for Ms. Szpindor. Unlike the House vendors, your office has no choice with regard to working with D.C. Health Exchange. Given what you know now about this breach and potential, I mean, this was an IP address totally exposed out there for God knows how long. What do you know about this breach? Does the D.C. Health Exchange meet the cybersecurity requirements of the House and its vendors? In other words, would the Exchange pass muster as a House vendor because we know that the CAO holds our vendors to a very, very high standard in terms of the applications we are allowed to use?

Ms. SZPINDOR. At the time we had our agreement with them put into place, the various agreements that we do have with them, it is hard to know if they would pass the evaluation since we really did not have an opportunity to do so. Certainly, if we were doing an evaluation now——

Ms. MACE. Would they pass muster today?

Ms. SZPINDOR. We would certainly have some questions, yes. We would have to reevaluate and probably ask some very hard questions on what had happened.

Ms. MACE. OK. Thank you, and I am going to yield to Mr. Connolly, 5 minutes.

Mr. CONNOLLY. Thank you, Madam Chairwoman. Ms. Kofman, how did you learn that customer data had been exposed on the publicly available website *BreachForums*?

Ms. KOFMAN. We work very closely with the city's technology agency, and one of their vendors identified the problem. The technology agency came to us on Monday around 12, and within 15 minutes, we confirmed that 11 of our customers' information was posted in this solicitation.

Mr. CONNOLLY. So, they brought it to you?

Ms. KOFMAN. The city technology agency we work with, correct, and then we immediately notified law enforcement, the FBI Cybersecurity Task Force, and asked them for assistance.

Mr. CONNOLLY. As I understand, the D.C. Capitol Police identified another website, *Pastehub.net*, where the hacker posted a sample of the purloin data. To your knowledge, did the stolen data appear on other publicly available websites, in addition to those two: *BreachForums* and *Pastehub*?

Ms. KOFMAN. Not to my knowledge, but that is also a question I am happy to follow up with law enforcement as well as the external experts we have.

Mr. CONNOLLY. During the early days of the data breach investigation, I guess by Mandiant, what steps did your office take to inform the appropriate entities of the breach to ensure that other potential targets received alerts as quickly as possible?

Ms. KOFMAN. We and the city technology agency immediately notified the U.S. Cybersecurity Infrastructure Security Agency, U.S. Homeland Security and Emergency Management Agency, we notified CMS, our oversight agency within the hour of learning of the breach. And we also, the next day, once we had confirmation that congressional information was in the stolen reports, we notified the House and Senate personnel offices, as well as OPM and others.

We took immediate steps for mitigation. And, well, we did two things. Mandiant within 2 days was able to identify the source of the breach, and we shut it down immediately. That was within 2 days of the breach. And within 3 days of the breach, we were able to secure identity theft and credit monitoring protection for 3 years for all three major credit bureaus. And that Thursday, March 9th, we notified 56,415 people whose information was stolen. And then that Friday, March 10th, we started to notify other people whose information was stored in the same manner that these stolen reports were stored in out of abundance of caution.

Mr. CONNOLLY. Were the people in that 56,000 population, they were told directly your data has been breached?

Ms. KOFMAN. Yes.

Mr. CONNOLLY. OK, because some of us got a generic notification that there had been this breach, but it was not clear that you personally were part of that. So, if you were not told directly, you were not affected?

Ms. KOFMAN. Correct. We wanted to notify others, and that is why you got a general notification saying the protection we have secured is available to you, your information was not breached, but we wanted to give you the same protection as we——

Mr. CONNOLLY. Right. Responsible, yes. Thank you. Ms. Szpindor, what is the relationship between your office and Ms. Kofman's? I mean, as you point out in your testimony, we are the only group that I know of required by law to go to the Exchange, and that Exchange is our local D.C. Exchange, and our staff, except Committee staff who have exempted themselves. So, what is your relationship with this office, and what is your view about their special relationship given the fact that we are a high target? We are kind of in the high-risk category. What is your response? What is their responsibility? What is your responsibility to be, you know, a careful guardian of pretty sensitive information about thousands of Capitol Hill employees?

Ms. SZPINDOR. Well, I have not talked to Mila frequently, but we certainly worked together when we were first setting up the Exchange, translations that we have to do in order to get them the data that they need. But primarily, we do not stay in close contact with each other because we have had the systems operating and functioning fairly well from our perspective, until this has happened over the past years.

But basically, what they do is we have access to a different type of system than the report system that they are talking about, their main healthcare system, where our Payroll and Benefits employees will initially enter into their system through the web interface that they have, the names of the individuals who are eligible to enroll in the D.C. Health Link data Exchange or D.C. Health Link Exchange. So, we have our staff that interfaces that to provide them names of individuals.

We also have, once someone decides they want to be or are going to be on the Exchange, our payroll and benefits system works with them to enter the information that they are going to be on the Exchange. And I think everything else then is carried forward by D.C. Health Link as far as reaching out to the employee, entering all

their detail, their personal information, and the healthcare plan that they are selecting.

Other than that, during the month, we have an interface between the CAO's technology group and their group whereby we send them any discrepancies that might have to be changed in their system and any other small issues that might come up, things that have to be corrected. That is sent through, what we have is a gateway server, which is just a very secure server where it is almost like, you open up the traffic so that the data that we want to send goes in. We know when they want to accept the data, we open it up just for them to be able to pull that data from the gateway server, then that connection is closed. So that is pretty much on a routine basis what we do.

Mr. CONNOLLY. OK. Thank you. My time has expired.

Ms. MACE. All right. I would now like to recognize Chairman Loudermilk for his 5 minutes.

Mr. LOUDERMILK. Thank you, Madam Chair. Thank you both for being here today. I must admit that being 30 years in the IT industry, I worked a lot to secure networks and worked for my customers to hack into their networks, and I have become more confused sitting in here today as to what happened. I thought it would be clarifying.

First of all, let me say, the majority of data leaks or cyber breaches are as the result of some form of human error. That is just known in the industry. When we work with companies, and I still will consult occasionally, without fee, to people who ask, especially when it comes to setting up a security policy, your first thing you do is understand the majority of your data breaches are going to come from some form of human error. In 2017, Equifax had one of the largest data breaches in our country's history. It was because of a human error, just because someone failed to apply a patch to a system that was critical for their cybersecurity. So, when I hear that it was a mistake, human error, tells me that there are other policies that were not in place to protect against these human errors, two-person integrity, double-checking what people are doing.

The other thing is an exposed IP address on itself does not create an exploitable server, many servers have through some form of firewall, gateway, IP masking, there is access to those servers that is needed. There had to be some other vulnerability that was exploited on that server.

So, before I get to my other questions, Ms. Kofman, I would like your commitment that you will provide this Committee the full Mandiant report as soon as it is received by D.C. Exchange because either they have either summarized at a very elementary level what happened, or we just need to know exactly. Will you provide that report to this Committee?

Ms. KOFMAN. You have Mandiant's incident report. In addition to that, what I am committing to doing is providing additional reports and information we gleaned from external, independent cybersecurity experts that I have asked to look at our entire system. To your point of processes, policies, looking at the entire AWS environment that we are in, looking at our firewalls, our code, our configurations. I am committing to providing you with updates on

what we learned from external experts we have hired and all the steps that we are taking to make sure this never happens again.

And we have tried, and I hope you recognize this, to be as transparent as possible and provide you with information as we have facts. I, myself, briefed six different congressional committees to date. We have met with——

Mr. LOUDERMILK. I do not mean to cut you off, but I am limited on time and I do have to get other things. We appreciate your transparency with us. We do not appreciate the transparency with the hackers, OK? Just from what I have heard in here today, I mean, every system is subjected to a hacker. When I ran a business, it was always the question was not if my customer is going to be hacked, but when, and you always had to stay a step ahead of the bad guy. It is vigilance. It is continual vigilance. That is the only way that you can secure against this. From just what I have seen so far, that this was made extremely easy for somebody to get in, but let me let me get to my questions at this point.

I want to start with Ms. Szpindor. Can you briefly describe for us the level of assessment a vendor must undergo prior to providing an essential service to the House that requires access to Member and staff data? Because a lot of times it is not just people inside the organization, but it is their vendors. What level of assessment must they go through?

Ms. SZPINDOR. We have a fairly rigorous process we put our vendors through. I can highlight some of the steps that we go through. We require an authorization to operate or ATO. That is managed primarily by our cybersecurity team with the help of the other groups that are in our technology organization. This is for contract-owned systems, systems hosted outside of the House infrastructure, enterprise cloud systems and third-party service providers and solutions or applications hosted on House infrastructure. There are two critical requirements.

The ATO process is to ensure that the vendor's implementation of security and privacy controls are there to protect the House information and is validated and monitored throughout the system lifecycle. The ATO process requires vendor-supported information systems to undergo an independent assessment to test and validate the implementation of security controls to protect the confidentiality, integrity, availability, and privacy of House information. A condition of the ATO approval is that the vendor system be enrolled in a continuous monitoring program to continuously assess and validate successful implementation and effectiveness of required security controls.

Mr. LOUDERMILK. Now, it sounds like it is not only do you give the access, but you are continuing to monitor their access.

Ms. SZPINDOR. We are.

Mr. LOUDERMILK. OK.

Ms. SZPINDOR. And if there were anything that would come up similar, some of the things that were brought up about VMware, SolarWinds, things of that sort, we knew a vendor might be using that product, we would immediately contact them and initiate some type of requested assessment.

Mr. LOUDERMILK. OK. Thank you very much. Ms. Kofman, same question. Briefly describe for us your level of assessment a vendor

must go through prior to providing service to the D.C. Health Exchange?

Ms. KOFMAN. Thank you. So for our vendors, we require that for their employees, that there is no civil or criminal activity related to—and I will just read you a portion relevant to this—"fraud, theft, embezzlement, breach of fiduciary responsibility or other financial misconduct in connection with the delivery of healthcare item, a service or with respect to any act or omission in any program operated by or financed in whole or in part by any Federal, state, or local government agency." So, our vendors are required to do due diligence on employees that they hire. For our own employees, we follow D.C. government standards, which include criminal background checks for security sensitive positions, which means fingerprinting, FBI fingerprinting, and criminal background.

Mr. LOUDERMILK. So, what I am hearing is you do a formal background check on your vendors and your employees. What I did not hear is the ongoing analysis of your vendors and their access to the systems and evaluating their systems as well.

Ms. KOFMAN. I just want to clarify, we do the background checks, working with another D.C. agency, for our employees. We require our vendors to be responsible for doing the checks on their employees. Otherwise, they are in breach of their contract with us.

Mr. LOUDERMILK. OK. I understand. I have gone way over my time. I yield back.

Ms. MACE. We all have, but appreciate your comments, Mr. Loudermilk, about the IP addresses—because it is exposed does not mean that the reports are right there, and if so, there is something obviously more going on here, and we are not getting the answers today on that "misconfigured" server.

I would now like to recognize Congresswoman Torres for her 5 minutes.

Mrs. TORRES. Ms. Szpindor, of the 56,000 individuals exposed outside of the Members of Congress and the staff, I think us working on this campus are very knowledgeable and have access to a lot of resources to protect our information. I am very concerned about the people outside of this campus. Can you tell me how did you notify them? Let us start with that.

Ms. SZPINDOR. And I want to be clear I understand, for those individuals whose data was exposed, but maybe they had been a House employee——

Mrs. TORRES. Had not been a House employee.

Ms. SZPINDOR. Had not been a House employee.

Mrs. TORRES. Just your average citizen that buys their——

Ms. SZPINDOR. Well, I understand, we did not notify those individuals. That was up to D.C. Health Link to notify those individuals that were not House employees.

Mrs. TORRES. OK. Can you answer that question, Ms. Kofman?

Ms. KOFMAN. Yes. So, we did it through a variety of mechanisms. One, within 3 days of the breach, we secured identity theft and credit monitoring protection through Experian for 3 years.

Mrs. TORRES. No, no, I understand that. How did you notify the people working outside of this building?

Ms. KOFMAN. Yes, we notified everyone.

Mrs. TORRES. How, email? Phone? Multiple languages? Only in English? Explain that to me.

Ms. KOFMAN. We put a notice in their D.C. Health Link account and triggered an email alerting them to review their notice that it is urgent. The notice had, in addition to English, had a bunch of other taglines associated with it. It was very clear saying their information was breached. We identified specifically which of their information was breached, and I will just tell you the take-up rate for Experian protection is now 19.1 percent. And I think that also——

Mrs. TORRES. That is still a very low number. Nineteen-point-one percent of the people that you notified have utilized, taken advantage of the resources that you are providing, is that correct?

Ms. KOFMAN. So, the average Experian reports is 5 percent to 10 percent. Another major Credit Bureau reports about 4 percent take up rate. So, I agree with you, it should be 100 percent, but it is higher.

Mrs. TORRES. Yes. I am just trying to get to how do we work together to ensure that we protect the people outside of this building. Those are the people that need our help the most. Those are most vulnerable, the day-to-day American who goes to work every day, who does not understand about the security issues, you know, that we face here in this building every day. What more can you do on that note to help those people?

Ms. KOFMAN. So, in addition to issuing three public updates, we briefed the three largest D.C. chambers asking them for help to notify their members. Many of their members are our customers, so D.C. Chamber of Commerce, the Greater Washington Hispanic Chamber of Commerce, and the Restaurant Association Metropolitan Washington. In addition to that briefing, we asked our brokers, we emailed our brokers, and we did two briefings for our brokers. Ninety-two percent of our employers have a broker, and we asked our brokers to notify their clients about this breach and asked for their help.

Mrs. TORRES. Did they do that, to your knowledge?

Ms. KOFMAN. I think some did.

Mrs. TORRES. OK. Can you follow up on that and let us know if that was done, and if not, I hope that you would, you know, go back to them and ensure that that gets done. My other question is, the server configuration concern, who provided the guidance for the person who configured that server? Did the people providing guidance on how that server needed to be configured, did they have a background in cybersecurity? Do we know that?

Ms. KOFMAN. So, everyone who works on our system has IT skill set, and then we have folks who look at the security aspect of the code and what they are doing.

Mrs. TORRES. And how often do they get training on security breaches and how to protect the system?

Ms. KOFMAN. The cybersecurity training for our staff and that our vendor has is just ongoing. There are formal things that they also must do, but it is ongoing. And if I can just add, I hired an external cybersecurity expert to investigate what happened with this human mistake. And we are going to have a lot of information on when the server was misconfigured, why it was misconfigured,

why it was not caught, and all of the steps that led to this event. And once we identify everyone who had any part of it, we are going to have lots of information to act on and lessons to make sure it never, ever happens again.

Mrs. TORRES. Thank you, and I yield back.

Ms. MACE. And hopefully that means they get fired. I am going to recognize Congressman Timmons for his 5 minutes. And then the witnesses asked for a break, and we will do that after Mr. Timmons questions for 5 minutes. We will do a quick 5-minute break, OK? All right, Mr. Timmons?

Mr. TIMMONS. Thank you, Madam Chairwoman. We have a problem in this country both with cybersecurity and privacy. It is not just the government. It is the private sector. We have not taken the steps necessary to protect the data that we either voluntarily give to private companies or involuntarily give to the government.

When a private company has a data breach, people file lawsuits. They have to do a settlement. There are fines. The largest settlement is $1.2 billion, $877 million, Equifax $575 million. So, that is how we hold them accountable. We hold them accountable by fining them, and the purpose of that is to get other businesses to take better care of their data and to protect their customers more.

We just found out a couple hours ago that the CFPB, which we do not voluntarily give our data to them, they take it, they acknowledged that they had a data breach. A quarter million individuals' files were sent in an email, and so the people that fine businesses—I mean the Equifax settlement was with the FTC and the CFPB. So, what are we going to do to them? And I guess that is one thing I want to talk about, but the other thing is this: your business is a public-private partnership. What is your ownership structure? Ms. Kofman?

Ms. KOFMAN. Yes. We were set up by D.C. Government as a private public partnership. What that means is we have a private executive board that oversees our policies and sets direction.

Mr. TIMMONS. I mean, if it is a public-private partnership, there is a private in there. So, is it a for-profit? Is it not-for-profit? Who owns it?

Ms. KOFMAN. It is an instrumentality of D.C. government, so it is quasi-government. I am sorry.

Mr. TIMMONS. So, it is quasi-governmental. Do you have statutory immunity? Could somebody sue you for this? Can you get a fine for this? What is going to happen? I mean, I am sure you have talked to your lawyers. What is going to happen, other than you have to come before Oversight and maybe have some changes to your contracts? What is going to happen? What do you think is going to happen?

Ms. KOFMAN. There have been lawsuits that have been filed.

Mr. TIMMONS. OK. By individuals or by the FTC, or who is coming after? Who is pursuing this?

Ms. KOFMAN. Affected individuals.

Mr. TIMMONS. OK. I imagine that it will be ongoing for a while. If you do get a fine and/or settle, how do you pay for that? Do you have insurance?

Ms. KOFMAN. We are required by Federal law to be self-sustaining and financially solvent. We have a capital reserve that we will be using if we have to.

Mr. TIMMONS. So, if you have to pay tens of millions of dollars to settle a lawsuit, you are going to then turn it around and charge your customers more? How are you going to do that? Is that the plan? Is that what would happen?

Ms. KOFMAN. You also asked whether there is cybersecurity insurance policy in place. There is one.

Mr. TIMMONS. What are the limits?

Ms. KOFMAN. I do not know.

Mr. TIMMONS. OK. Well, I mean, I do not think many people have an option other than to use your services. I am pretty sure that I have to. I mean, Members of Congress are on that Exchange and we are statutorily required. That was a great idea that Congress did during Obamacare. But, you know, we got to have accountability. And we have accountability with Equifax and Amazon when they have these breaches. They pay huge sums of money, and I guess I just hope that your cybersecurity insurance is sufficient to cover whatever damages are deemed to have. I guess, Ms. Szpindor, do you think that we should reevaluate whether Members of Congress and your employees should be forced to use the health exchange?

Ms. SZPINDOR. Well, I really think that that is up to you in Congress to make an evaluation of that. We were compelled to do so.

Mr. TIMMONS. By the law?

Ms. SZPINDOR. By the law and through OPM, who said we would use the D.C. Health Exchange to facilitate the Members and any of their staff from joining, but I think that that is definitely something that is up to the Members.

Mr. TIMMONS. OK. I appreciate that answer. Thank you, and, Mr. Chairman, I yield back.

Ms. SZPINDOR. Thank you.

Ms. MACE. Thank you. And we are going to just let you take a 5-minute break and we will be here when you are done. All right.

[Recess.]

Ms. MACE. All right. Now that we are back in order, I would like to recognize our esteemed colleague, Ms. Norton, for her 5 minutes.

Ms. NORTON. I thank the Chair, and I thank her for this hearing. I also would like to thank our D.C. witnesses for being here this day, today. To begin, I would like to note that while this data breach is deeply concerning, it is not unique to D.C. Director Kofman, do you agree this breach is not unique to the District of Columbia?

Ms. KOFMAN. Yes.

Ms. NORTON. That, of course, is correct. The private sector and Federal, state, and local governments across the country, including governments and all the states represented by all the Republicans on both Subcommittees here today, have experienced data breaches. For example, Kentucky's health insurance program for government employees and retirees suffered two data breaches in 2020.

As we have discussed, the breach of D.C. Health Link allowed the theft of sensitive personal data, jeopardizing the physical safety

and financial security of more than 50,000 people. It also put the data of almost 200,000 additional people at risk of theft. Many of the victims are D.C. residents, families, small businesses, and nonprofits that I represent. Ms. Kofman, you mentioned that the D.C. Health Benefit Exchange Authority is offering 3 years of free credit monitoring to all customers whose data was at risk. How do these resources or resource offerings compare to what other breached organizations offer victims?

Ms. KOFMAN. Yes. We believe that the 3-years of identity theft monitoring and credit monitoring for all three major credit bureaus for 3 years exceeds what typically happens. Typically, you may get one or 2 years, or you may just get monitoring for one major credit bureau. We wanted to go as broad as possible and beyond people whose information was not stolen. We have made this protection available to everyone, past and current customers.

Ms. NORTON. Well, Ms. Kofman, once you discovered the breach, how quickly were these resources offered?

Ms. KOFMAN. We discovered the breach on March 6. We were able to secure Experian credit monitoring and identity theft monitoring by March 9, and that is when we notified the customers whose information was stolen. And then on March 10, so this is just a matter of days after discovering the breach, on March 10, we started to notify other customers whose information was stored in the same manner as the two stolen reports, but we had no evidence that it was actually stolen.

Ms. NORTON. I understand that the acceptance rate for credit monitoring and other services you offered were higher than the industry average. Mr. Kofman, have you considered taking any additional actions to support victims of a data breach?

Ms. KOFMAN. Yes. We continue to work with all of our D.C. Health Link assisters and the three largest chambers and certainly our brokers. We have asked them for help to notify their clients. I also just want to say how appreciative I am of the House CAO and her deputy in the outreach that they did through their mechanisms to Members of Congress and affected staff.

Ms. NORTON. Well, Ms. Kofman, did D.C. Health Link inform affected customers of the breach and of the credit monitoring resources by our message loaded into the D.C. Health Link account inboxes. Isn't that correct?

Ms. KOFMAN. We loaded the breach notice into D.C. Health Link account and that also triggered an email to let the person know to check their account.

Ms. NORTON. This message generated a generic email to email addresses on file, notifying them to check their D.C. Health Link account box. Is that correct?

Ms. KOFMAN. Yes.

Ms. NORTON. Did the email contain any mention that the breach had occurred or give any indication that their personal data had been compromised?

Ms. KOFMAN. The email itself did not have that kind of information. It was marked "urgent" for them to check their D.C. Health Link account for an important notice.

Ms. NORTON. I see. Impacted individuals would therefore need to take the time to log into their D.C. Health Link accounts to even

know about the breach and the free credit offering, isn't that correct?

Ms. KOFMAN. Yes, they can also call our call center and get that information as well. We shared information with the three largest chambers and our brokers so our brokers can share that information with their customers. And, so, we have different ways that we have shared both the Experian codes and the information on how to sign up for the 3-year protection.

Ms. NORTON. We understand, Ms. Kofman, that the open rate for emails was between 22 percent and 32 percent. So theoretically, many individuals impacted by the breach are not aware that their data was stolen.

Ms. KOFMAN. The open rates for the notices, I think, is what you quoted. That is how many people actually looked at the notice. And, so, we are not relying solely on the email or the information in the account, and that is why we did three public updates and we created a special web page on *dchealthlink.com*. Initially, we had a pop-up, so that is the first thing you see when you go to *dchealthlink.com* that we suffered a data breach. But that is precisely why we are working with stakeholders, like the business community and our brokers and our D.C. Health Link-certified assisters to help get the word out and encourage people to avail themselves of the 3-year identity theft and credit monitoring protection for all three major credit bureaus.

Ms. NORTON. Well, Ms. Kofman, has the authority explored a digit——

Ms. MACE. Ms. Norton, we are about two-and-a-half minutes over.

Ms. NORTON. I know, but everybody——

Ms. MACE. Everybody got about two-and-a-half minutes over.

Ms. NORTON. OK.

Ms. MACE. Well, you and Timmons did not, so. About 30 more seconds, please.

Ms. NORTON. Well, I must note that everybody took more time, and since I am more deeply involved than everyone else——

Ms. MACE. No. Yes, ma'am, and I am giving you more time. You are at almost 3 minutes over.

Ms. NORTON. All right. OK.

Ms. MACE. Which will be the most that anybody had today, so thank you.

Ms. NORTON. All right. I am almost through. Ms. Kofman, has the authority explored additional methods of notifying D.C. residents besides email, such as text, phone call, or paper mail?

Ms. KOFMAN. We are looking at all options available to help notify people.

Ms. NORTON. Finally, Ms. Kofman, what metrics and evaluative tools are you using to assess the effectiveness of your outreach strategies?

Ms. KOFMAN. Well, we looked at the industry, what Experian and other major credit bureaus report for take-up rates in case of breaches, and Experian reports 5-to 10-percent take-up rate. Ours is currently is 19.1 percent, so above their reported average. Equifax reports 4 percent take-up rate. So right now, we are at 19.1 percent, but as I mentioned earlier, obviously we want every-

one whose information was stolen to avail themselves of this protection.

Ms. NORTON. Thank you.

Ms. MACE. Thank you, Ms. Norton. I would now like to recognize Congressman Steil for 5 minutes maybe.

Mr. STEIL. I will try to keep it at 5. This is an important topic. Chair Mace, Chair Loudermilk, thanks for doing this, the Ranking Members as well, Ms. Szpindor, Ms. Kofman for being here and going through this.

Last month, Members of the congressional community, including over 800 House Members, staff, and family members, at a minimum had their private information unnecessarily exposed after the breach of the D.C. Health Link. To me, the goal of our hearing today is how did this happen, what steps are being taken to protect the information of those exposed, and ensuring it never happens again. We received the seven-page forensic report. Ms. Kofman, did I hear you that that is the final report or is that the preliminary report?

Ms. KOFMAN. The report we shared with the Committee staff is Mandiant's incident report.

Mr. STEIL. Yes, and that is not the preliminary report, that is the report?

Ms. KOFMAN. I believe that is the report on the incident.

Mr. STEIL. Let me then come in. I thought it was the preliminary report when I read it. It is seven pages. It is wildly underwhelming if that is the final report. I think that is something we will look into more broadly. Go ahead, Ms. Kofman.

Ms. KOFMAN. So, in addition to the getting Mandiant in right away to help us with the incident response, and that is the report you have, I have asked external cybersecurity experts to look at our entire system, which includes looking at our code, looking at the AWS environment to make——

Mr. STEIL. So, see if I get this correct. So, there is another vendor separate of Mandiant that is producing this review?

Ms. KOFMAN. We have several different expert vendors who are looking at our entire system. And what I have committed to doing earlier is providing you with information as we have information from external experts who are looking at our entire system to make sure, one, there is no malicious actor in our system——

Mr. STEIL. Understood. I got a lot of questions and, I do not know if I have a short amount of time, but a short amount of time to go through this, so I appreciate that. I will just say that the Mandiant report was wildly underwhelming. I will leave it there for now. You noted, I think, Ms. Kofman, you said to Ms. Mace that this vulnerability may have existed for 5 years. Is that accurate?

Ms. KOFMAN. The server in question was misconfigured mid–2018 when it was being configured to work with Slack.

Mr. STEIL. So, you will say misconfigured, I will say vulnerable, but the problem existed since 2018?

Ms. KOFMAN. We are figuring out when exactly the issues occurred.

Mr. STEIL. OK.

Ms. KOFMAN. But the configuration was done in mid–2018, and so another external expert on cybersecurity is doing a full investigation for me to identify all those facts.

Mr. STEIL. Understood, and I appreciate that. Ms. Szpindor, I appreciate you being here. How often is the House of Representatives the target of a cyberattack?

Ms. SZPINDOR. Every single moment of every day.

Mr. STEIL. Continuously?

Ms. SZPINDOR. Continuously.

Mr. STEIL. Every moment, every day, we are the target of attacks. The CAO's Office of Cybersecurity works around the clock to ensure to protect Members and staff that our data is protected. Is that accurate because we are getting attacked around the clock.

Ms. SZPINDOR. Yes, sir. It is all the cyber team plus me to——

Mr. STEIL. And I appreciate and let me say, I know you got a lot of folks on your team that do a great job on behalf of both the staff and the Members here, and thank you to you and your staff for the work you guys do literally around the clock in particular as it relates to IT. Any vendor wishing to do business with the U.S. House of Representatives, it has got to go through a vigorous and rigorous assessment by the CAO in order to be approved and granted access to our systems. Is that correct?

Ms. SZPINDOR. Correct.

Mr. STEIL. And would a vulnerability exist for years in the House? Would a vulnerability be able to exist for years before it is detected?

Ms. SZPINDOR. I would think it would be very, very hard to have a vulnerability out there that we would not detect for that length of time.

Mr. STEIL. Yes. OK. So, I mean it is obviously, in theory it is possible, but we got a really rigorous system here in the House. We do not think that happens because we have systems in place that we would catch it.

Ms. SZPINDOR. Yes.

Mr. STEIL. And that is why we have a high standard. And the breach that occurred did not occur in any system under your control the U.S. House of Representatives, right?

Ms. SZPINDOR. That is correct.

Mr. STEIL. And, so, the PII that is out there was because there was a vendor that was not vetted by the U.S. House Representative system, right?

Ms. SZPINDOR. Correct.

Mr. STEIL. And Members and staff are required to participate in this Exchange due to a law that was written by Congress, a Federal law. Is that right?

Ms. SZPINDOR. Correct.

Mr. STEIL. And, so, the breach that occurred, occurred on a vendor that does not meet the House's standards. Is that accurate? The standard that the vendor had and the error the vendor had would not meet the standard that you have for vendors to the U.S. House of Representatives, right?

Ms. SZPINDOR. With this current breach.

Mr. STEIL. OK. And, so, Ms. Mace asked, Ms. Szpindor, if I can, as the Chief Information Officer of the House and the current CAO,

knowing what you do about cybersecurity practices of the D.C. Health Exchange Authority and the vulnerability that led to this breach, would you recommend D.C. Health Exchange Authority as a secure vendor with which the House could confidently do business?

Ms. SZPINDOR. I am not sure that I would——

Mr. STEIL. Well, they are below your standards, so I cannot fathom you would recommend that we would do this with them.

Ms. SZPINDOR. If we were doing an evaluation today.

Mr. STEIL. If you did an evaluation today of the standard that existed before the breach, would they pass or fail? They would fail.

Ms. SZPINDOR. Right.

Mr. STEIL. Right?

Ms. SZPINDOR. Right.

Mr. STEIL. But Members are still doing business with the D.C. Health Exchange today. I will tell you as Chairman of the Committee on House Administration, I look forward to working toward solutions to ensure that we serve this institution, and we are not in this position ever again. I appreciate our witnesses being here. Madam Chair, I yield back.

Ms. MACE. Thank you. I would now like to give 5 minutes to Congressman Griffith.

Mr. GRIFFITH. I thank the gentlelady, and I apologize that I have not been able to participate and be a part of this hearing up to this point in time. I was chairing another subcommittee hearing where we were dealing with issues related to data brokers. But this is an important hearing, and I look forward to getting all the information, not just the part I have been able to sit in on for the last, say, 15 minutes. With that, I would yield my time to my colleague from the great state of Georgia, Mr. Loudermilk.

Mr. LOUDERMILK. I appreciate that from my friend and colleague from Virginia. And I am going to try to keep this within our timeframe, so we can actually set a record in here that somebody stayed within the 5-minutes. And I just want to complete some of the questioning that I was doing earlier. Ms. Szpindor, as I know, but as you can explain, the House employs a number of information systems officers, is that correct?

Ms. SZPINDOR. Correct.

Mr. LOUDERMILK. Can you please elaborate on the role of these individuals as it relates to, as you mentioned, continually monitoring House-approved vendors?

Ms. SZPINDOR. Yes, I will be glad to. The individuals that we have that work within our cybersecurity group that are known as security systems officers, there are five of them. And they are essentially responsible for when a request comes in from a vendor, and we are beginning the ATO process to determine their viability as a vendor. They make sure that all the steps are followed, that we have done the evaluation as it was intended to be done, and these individuals work around the clock. So far, we have authenticated 36 different systems and have nine in progress. But these ATOs are reevaluated on a continuous basis, so these individuals stay very busy.

Mr. LOUDERMILK. So, in short, you may say that they are always checking the work?

Ms. SZPINDOR. Yes.

Mr. LOUDERMILK. OK.

Ms. SZPINDOR. And by the way, we are talking about our PeopleSoft system and some of our other large systems that we have as well as part of that.

Mr. LOUDERMILK. OK. Thank you for that. Ms. Kofman, does the D.C. Health Exchange have information system security officers on staff?

Ms. KOFMAN. We do, and may I address something else? There has been a lot of assertions, many assertions made about how secure our system is. Let me just say we use Cloudflare, FortiGate, Splunk, Tenable, and other security technologies that U.S. intelligence agencies use, Fortune 100 companies use, U.S. Secret Service, Homeland Security, and the list goes on. We have 24/7 monitoring. We have been under attack since we opened for business October 1, 2013.

Mr. LOUDERMILK. I understand that, and that is an impressive list. But the fact remains there was a breach, that it goes to the security in the operations, having those systems, having those devices, just as Equifax learned, unless they are continually monitored, unless the oversight is given, unless the policies and procedures that you have address potential human error and that they are enforced, you are going to have these types of breaches. I want to continue on my questioning though. You said, yes, that you do have information system security officers on staff, how many?

Ms. KOFMAN. Correct. In addition to an outside firm we use to help us with 24/7 monitoring of our system, we have full-time people. We have four people on staff who work in addition to the outside firm we use.

Mr. LOUDERMILK. Those four people, they are considered information systems security officers, not just IT folks, not just programmers, not just network analysts, they are specifically for security?

Ms. KOFMAN. They only work on cybersecurity.

Mr. LOUDERMILK. OK. And, so, you have four, and you said a vendor?

Ms. KOFMAN. And we use supplemental staff from a cybersecurity company to supplement the four, and then internally, when we need to pull in more people, we do.

Mr. LOUDERMILK. So, do these four that you have alluded to, do they continually monitor and test your vendors for cybersecurity vulnerabilities?

Ms. KOFMAN. Yes, they test everything. They look at the code, they look at the environment, they engage in pen testing. They look at, you know, the 24/7 logs we get.

Mr. LOUDERMILK. Do they look at server configurations?

Ms. KOFMAN. They look at everything.

Mr. LOUDERMILK. But something got missed?

Ms. KOFMAN. Something got missed, and that is why I wanted an external investigator to help me figure out how we missed this, why it was missed, so it never gets repeated again.

Mr. LOUDERMILK. Well, since Mr. Griffith took about 45 seconds to yield to me, I technically made it within my time. I yield back to Mr. Griffith.

Ms. MACE. Thank you.

Mr. GRIFFITH. And I yield back to the Chair.

Ms. MACE. Thank you. In closing today, as we wrap this up, I want to thank our panelists once again for their testimony today and those Members of Congress who showed up and asked tough questions. I appreciate the witnesses' participation and willingness to discuss the data breach at the D.C. Health Exchange. Questions remain. We still do not know what a misconfigured server by D.C. Health Link standards is. We know when it was misconfigured. We do not know who misconfigured it or how it was misconfigured, and the Mandiant report was pretty lame and uninformed. So, Ms. Kofman, I hope you and your team will continue to cooperate with Congress and with this Committee. Please keep us posted about any future reports related to the data breach and actions taken by the Exchange in response to the breach. Will you commit to that?

Ms. KOFMAN. Yes.

Ms. MACE. With that and without objection, all Members have 5 legislative days within which to submit materials and submit additional written questions for the witnesses which will be forwarded to the witnesses for their response.

Ms. MACE. If there is no further business, without objection, we are adjourned.

[Whereupon, at 4:34 p.m., the Subcommittees were adjourned.]

○