DC Health Benefit Exchange Authority

JOINT HEARING BEFORE THE UNITED STATES HOUSE OVERSIGHT AND ACCOUNTABILITY SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION AND HOUSE ADMINISTRATION SUBCOMMITTEE ON OVERSIGHT

April 19, 2023

Testimony of Mila Kofman, Executive Director of the District of Columbia Health Benefit Exchange Authority

Good afternoon Chairwoman Mace, Chairman Loudermilk, Ranking Member Connolly, Ranking Member Torres, Representative Norton, and Members of the Committees. Thank you for the opportunity to testify before you today. My name is Mila Kofman and I am the Executive Director of the District of Columbia Health Benefit Exchange Authority ("DCHBX").

As background, the District of Columbia government established DCHBX as a private-public partnership, with a private Executive Board, to implement the federal health care law to promote transparency, competition, and help residents, families, and employers to have health coverage that works for them. DCHBX built and operates DC Health Link, the District's state-based online health insurance marketplace. DC Health Link was one of four state-based marketplaces to open for business on time, on October 1, 2013. DC Health Link has more than 200 health plan options with nationwide and local networks from major health insurance companies including Aetna (group only), CareFirst Blue Cross Blue Shield, Kaiser Permanente, and United Healthcare (group only). These plans include PPO, HMO, and POS options that range from zero deductible options to HSA High Deductible Health Plans. We are responsible for more than $670 million in annual premiums. Since opening, we have cut the uninsured rate by half. Over 96% of DC residents now have healthcare coverage. The District ranks number two in the United States for the lowest uninsured rate.

Today I am here on behalf of DCHBX and our Executive Board to discuss DC Health Link data breach affecting 56,415 current and past customers including members of Congress, their families, and staff. As you know, on March 6, 2023, we learned that a threat actor stole personal data from DC Health Link. While DC Health Link does not have medical or health care information, we do have sensitive personal information. The two stolen reports had personal information including name, date of birth, and social security numbers.

In addition to saying how sorry I am that 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. When we learned of the breach, we immediately asked the FBI Cyber Security Task Force for help and

engaged a leading cyber security incident response firm, Mandiant. Mandiant identified the source of the breach and DCHBX staff shut it down immediately. We also acted quickly to notify and help protect affected people by immediately offering them identity theft and credit monitoring services. As shared with your staff, I also immediately asked third-party cyber security 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. And with strong support of our Executive Board, we've made and will continue to implement changes to better protect DC Health Link and our customers from threat actors and from criminals looking to steal personal information of DC Health Link customers.

TIMELINE

On March 6, 2023, we learned that intruders stole personal data of DC Health Link customers and exposed the data of 11 of those customers on Breached Forums. The next day, we notified the 11 people whose information was included in the threat actor's advertisement and offered them three years of identity theft and credit monitoring protection from all three major credit bureaus. We immediately asked the FBI Cyber Security Task Force for help. Two special agents from the FBI Cyber Security Task Force were in our offices that afternoon to help us. We also engaged Mandiant, an independent cybersecurity forensic consulting firm, and launched an investigation.

On Tuesday, March 7, 2023 law enforcement obtained the reports and that afternoon provided our team with the two DC Health Link reports that were stolen. The stolen data included that of 17 Members of the House and 43 of their dependents, and 585 House staff members and of their 231 dependents.

On Wednesday, March 8, 2023, Mandiant, working with our security team, identified the source of the breach. Our security manager immediately shut it down. Also, we completed our review of the two stolen reports. It took our team approximately 24 hours to go through the two stolen reports, validate, and deduplicate the data. While our security team was working around the clock to identify the breach and shut it down and our IT team reviewed the two stolen reports, we were also working to procure identity theft and credit monitoring protection for affected current and former customers.

On Thursday, March 9, 2023, we procured 3 years of identity-theft and credit monitoring protection for all three major credit bureaus for our affected customers. This coverage also protects dependents, spouses, and children. As soon as Experian provided us with a toll-free number and generated codes for our customers to use to sign up, we notified the 56,415 customers whose data we knew had been stolen. We loaded a notice into their DC Health Link account and emailed customers to let them know about the data breach notice in their account. We chose to have Experian generate a general code instead of a unique code for each customer because generating a unique code would have required an additional 3 to 5 days—we wanted to get this protection in place immediately. In addition, Mandiant and DC Health Link's security team continued to analyze forensic data. Through this effort, we identified data that was stored in the same manner as the two stolen reports. Although there was no evidence that

additional data outside of the two stolen reports was stolen, out of abundance of caution, we offered the same 3 years of identity-theft and credit monitoring protection services to those customers, notifying them on a rolling basis beginning on Friday, March 10, 2023.

FEDERAL NOTIFICATIONS

I want to say how much DCHBX appreciates how quickly the FBI Cyber Security Task Force responded to our request for help. Their guidance allowed us to prioritize transparency and to share information with our customers as quickly as possible.

On March 6 and 7 (the day we discovered the breach and the day after), DCHBX and the DC Office of the Chief Technology Officer notified or briefed federal agencies, as required. Also, through notifications of regulatory bodies and law enforcement, we sought to understand the available resources and help as we worked to address the incident. We notified:

- Cybersecurity & Infrastructure Security Agency (CISA),
- US Homeland Security & Emergency Management Agency,
- FBI Cyber Security Task Force,
- Centers for Medicare & Medicaid Services (withing 1 hour of discovering the breach as required by federal law),
- U.S. House of Representatives, Office of the Chief Administrative Officer. I want to thank both Catherine Szpindor and James Butler for their help in responding to our data breach.
- U.S. Senate, Senate Disbursing Office,
- Office of Personnel Management (OPM), and
- Multi-State Information Sharing and Analysis Center (MS-ISAC).

OUR COMMITMENT TO TRANSPARENCY

We provided public updates on March 8, March 10, and March 14. We set up a dedicated webpage on DCHealthLink.com that has these updates and Frequently Asked Questions.

In addition, we briefed the US House of Representatives Committees on House Administration, Energy & Commerce, and Oversight & Accountability, and the US Senate Committees on Health, Education, Labor & Pensions, Homeland Security & Governmental Affairs, and Rules & Administration. And on a personal level, I would like to express my gratitude to House CAO Catherine Szpindor and her deputy James Butler for the help they have provided us in reaching the Members and staff affected by the data breach.

We've also briefed the DC business community and others we work with. For example, we briefed the three largest DC chambers including the DC Chamber of Commerce, the Greater Washington Hispanic Chamber of Commerce, and the Restaurant Association Metropolitan Washington – many of their members are enrolled in DC Health Link coverage. We held two webinars for our DC Health Link brokers, asking them to help alert their employer clients. We also briefed our DC Health Link assisters, who work with residents and their families.

In response to the data breach, we acted quickly to both immediately secure our systems and provide identity theft and credit monitoring protection to DC Health Link customers, their dependents, spouses and children. In addition, we made that same protection available to all other customers, including those not affected.

We asked law enforcement for help immediately and shared information as we uncovered it. Mandiant quickly worked alongside our team to identify the root cause of the breach, which we immediately eliminated. In addition to addressing this issue, we initiated a comprehensive review of our entire system and security, and we will be making enhancements across the board and can keep you updated on that progress.

MANDIANT INCIDENT REPORT AND INFORMATION ABOUT THE ROOT CAUSE OF BREACH

On Friday, April 14, 2023, Mandiant completed its incident response report. We have reviewed their findings. Per your staff's request, we have shared the report with your staff. We are still conducting our own investigation and are committed to updating you as that investigation proceeds.

Let me be clear at the outset: the cause of this breach was human mistake. With respect to the "root cause" – the problem here related to the configurations on a server used for generating and storing automated jobs and weekly reports. The server was misconfigured to allow access to the reports on the server without proper authentication. Based on our investigation to-date, we believe the misconfiguration was not intentional but human mistake. Also, at no point, was the DC Health Link enrollment system breached or exposed.

We have a strong cybersecurity program. For example, we use technologies such as FortiNet & FortiGate, CloudFlare, Splunk, and Tenable Nessus – many of which are used by the U.S. military and intelligence agencies, U.S. Department of Homeland Security, U.S Secret Service, Department of Defense, and Fortune 100 companies. We have successfully repelled attacks on our network and our site. In our early years, we faced a weeklong attack aimed at crashing our system (we faced approximately 100G traffic DDoS attacks and that was almost 100,000 requests per second). Since then, the number of attacks has fallen, but their sophistication has increased. On an average day, there are 2,000 malicious attacks. On December 9, 2020, we blocked 560,000 malicious attacks.

Again, what occurred here was the result of a human mistake, a mistake made in setting up a server used for storing and transmitting reports that were being used for business purposes.

In responding to the data breach, we implemented a series of remediation actions, and as I've explained, we are working with third-party cybersecurity experts to assess and further improve the security of the entire environment.

CONCLUSION

I want to reaffirm to Congress, to all enrollees of DC Health Link, and to the public at large, our commitment to ensuring access to quality and affordable health insurance coverage to all District residents, families, and employers.

We are not shying away from this breach. We have been and remain committed to being open and transparent. If your constituents need or request additional specific information, let us know. We want customers who were affected by this breach or who think they might have been by it to know what happened and to be fully aware of the protections we are offering them so that they can as quickly as possible enroll in the 3- year identity theft and credit monitoring protection.

I want to reiterate how deeply sorry we are that two reports were stolen with personal sensitive data of 56,415 past and current customers. We are making every effort to ensure this does not happen again.

I am happy to take your questions and if I can't answer some now, I will do my best to get you the information you need to protect the American people from this type of data theft.

Thank you for inviting me to speak today.