

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

JENNI SUHR, individually and on behalf all
others similarly situated,

c/o Mason LLP
5335 Wisconsin Ave. NW, Ste. 640
Washington, D.C. 20015-2052

Plaintiff(s),

v.

DISTRICT OF COLUMBIA HEALTH
BENEFIT EXCHANGE AUTHORITY,
d/b/a DC Health Link,

1225 Eye Street NW, Ste. 400
Washington, D.C. 20005

Defendant.

CASE NO. 1:23-cv-00694

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff(s) Jenni Suhr (“Plaintiff(s)”) bring this action on behalf of themselves and all others similarly situated against Defendant District of Columbia Health Benefit Exchange Authority, d/b/a DC Health Link (“DCHL” or “Defendant”). Plaintiff(s) seek to obtain damages, restitution, and injunctive relief for a class of individuals (“Class” or “Class Members”) who are similarly situated and have received notices of the data breach from DCHL. Plaintiff(s) make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of a 2023 data breach (“Data Breach”) of documents and information stored on the computer network of DCHL, an entity that holds itself out as helping individual, family and small business clients find quality health insurance coverage that meets their

needs and budgets.¹ DCHL was created “to implement a health care exchange program in the District of Columbia in accordance with the Affordable Care Act (ACA), thereby ensuring access to quality and affordable health care to all DC residents.”²

2. On its computer network, DCHL holds and stores certain highly sensitive personally identifiable information (“PII” or “Private Information”) of the Plaintiff(s) and the putative Class Members, who are individuals seeking and/or enrolling in health insurance benefits administered by DCHL, i.e., individuals who provided their highly sensitive and private information in exchange for employment and/or business services.

3. According to recent news reports and its Data Breach Notice Letters (*see* Plaintiff’s “Notice Letter” attached as Exhibit A), DCHL first became aware of the Data Breach on March 6, 2023 and began investigating.³

4. DCHL will be required to begin notifying the unknown or undisclosed number of victims as soon as possible stating that their PII had been stolen in this Data Breach. Although DC Health Link’s website states that the breach affected just over 56,000 customers’ data,⁴ an involved criminal entity was attempting to sell on the dark web the personal data of over 170,000 individuals from this Data Breach.⁵

5. DC Health link is the health insurance exchange that Congressional office are required to use in order to provide insurance for members and the staff.⁶

¹ <https://dchealthlink.com/brokers/overview> (last accessed Mar. 13, 2023).

² <https://dchealthlink.com/welcome> (last accessed Mar. 13, 2023).

³ <https://wtop.com/dc/2023/03/congress-members-warned-of-significant-health-data-breach/>; *See also* Pl.’s Notice Letter, Ex. A.

⁴ <https://dchealthlink.com/> (last accessed Mar. 13, 2023).

⁵ *See* <https://thecyberexpress.com/dc-health-link-data-breach-170000-pii-at-risk/> (last accessed Mar. 14, 2023); *see also* <https://www.cbsnews.com/news/data-breach-washington-dc-health-link-user-data-sold-dark-web-congress/> (last accessed Mar. 14, 2023).

⁶ <https://thehill.com/homenews/house/3890593-congressional-health-program-suffers-significant-data-breach-affecting-hundreds-of-lawmakers-staff/> (last accessed Mar. 14, 2023).

6. This Data Breach has affected the PII of members of the United States Congress and their family members, as well as thousands of other people, by publicly releasing their name, Social Security number, date of birth, gender, health plan information (e.g., plan name, carrier name, premium amounts, employer contribution, and coverage dates), employer information, enrollee information (e.g., address, email, phone number, race, ethnicity, and citizenship status) on the dark web.⁷

7. As news agencies have reported, a letter sent to House members stated: “This breach significantly increases the risk that Members, staff, and their families will experience identity theft, financial crimes, and physical threats—already an ongoing concern.”⁸ And these news reports suggest that this highly sensitive personal information has already been sold on the black market.⁹

8. As a result of DCHL’s Data Breach, Plaintiff(s) and thousands of Class Members suffered ascertainable losses in the form of financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

9. In addition, Plaintiff(s)’ and Class Members’ highly sensitive personal information—which was entrusted to Defendant—who claims in its Privacy and Security webpage (“Privacy Policy”) that “consumer privacy is important to us” and that “We respect your right to privacy and will protect the information we maintain about you in the ongoing operation of the health benefit exchange [omitted] in accordance with applicable laws, regulations and standards for security and privacy”¹⁰—was compromised and unlawfully accessed and extracted during the

⁷ See *id.*; see also <https://dchealthlink.com/> (last accessed Mar. 14, 2023).

⁸ <https://www.cbsnews.com/news/data-breach-washington-dc-health-link-user-data-sold-dark-web-congress/> (last accessed Mar. 14, 2023).

⁹ *Id.*

¹⁰ <https://dchealthlink.com/privacy> (last accessed Mar. 13, 2023).

Data Breach.

10. Based upon DCHL'S website notification and its notice letter, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-criminals who perpetrated this attack and remains in the hands of those cyber-criminals.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff(s) and Class Members' Private Information.

12. Plaintiff(s) bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

13. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

14. Defendant disregarded the privacy and property rights of Plaintiff(s) and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available

steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members prompt and accurate and complete notice of the Data Breach.

15. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the intrusion sooner and prevented access to the Private Information, and potentially been able to mitigate the injuries to Plaintiff(s) and the Class.

16. Plaintiff(s)' and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiff(s) and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during

the Data Breach (the “Class”).

21. Accordingly, Plaintiff(s) bring this action against Defendant for negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for DCHL’s unlawful conduct.

22. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant’s data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

23. Plaintiff Jenni Suhr is and at all times relevant to this Complaint an individual citizen of the State of Colorado, residing in the city of Littleton. Plaintiff Suhr is a benefits receiver through DC Health Link.

24. DC Health Link is governed by the DC Health Benefit Exchange Executive Board appointed by the Mayor of the District of Columbia and confirmed by the District of Columbia Council. The DC Health Benefit Exchange’s principal place of business is located at 1225 Eye Street, NW, Suite 400, Washington, DC 20005. Defendant can be served through the Mayor’s Office of Legal Counsel, at 1350 Pennsylvania Ave, NW, Suite 407, Washington, DC 20004.

III. JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

26. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business

venture in the District of Columbia; it maintains its headquarters in the District of Columbia; and committed tortious acts in the District of Columbia.

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district in which DCHL has the most significant contacts.

IV. STATEMENT OF FACTS

Nature of Defendant's Business

28. DCHL was created and is governed by the DC Health Benefit Exchange Authority, which “was established as a requirement of Section 3 of the Health Benefit Exchange Authority Establishment Act of 2011, effective March 3, 2012 (D.C. Law 19-0094). The mission of the DC Health Benefit Exchange Authority is to implement a health care exchange program in the District of Columbia in accordance with the Affordable Care Act (ACA)[.]” Its goal is to ensure “access to quality and affordable health care to all DC residents.”¹¹

29. DCHL claims “DC Health Link offers health insurance from 3 UnitedHealth Companies, 2 Aetna Companies, CareFirst BlueCross BlueShield, and Kaiser. Approximately 100,000 people have private health insurance through DC Health Link and this includes more than 5,000 District small businesses, approximately 11,000 designated Congressional staff and Members of Congress, and thousands of District residents.”¹²

30. Many of DCHL’s customers are employees of businesses located within the District of Columbia, including Members of Congress and their staff and Plaintiff here, but do not personally reside in the District and/or are not citizens of the District of Columbia.

31. DCHL, in the regular course of its business, collects and maintains the Private Information of individuals as a requirement of its business practice.

¹¹ <https://dchealthlink.com/welcome> (last accessed Mar. 14, 2023).

¹² <https://hbx.dc.gov/node/316092> (last accessed Mar. 14, 2023).

32. The individual consumers who seek the services of DCHL provide their Private Information with the mutual understanding that this highly sensitive private information is confidential and will be properly safeguarded from misuse and theft.

33. DCHL promises in its Privacy Policy to “Please be assured that this site is equipped with security measures to protect the information you provide us. [DCHL claims it] encrypt[s] credit card numbers and other data that must remain secure to meet legal requirements.”¹³

34. In the course of collecting Private Information from consumers, including Plaintiff(s) and Class Members, DCHL promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. DCHL is aware of and had obligations created by the FTCA, contract, industry standards, and common law to keep Plaintiff(s)’ and Class Members’ Private Information confidential and to protect it from unauthorized access and disclosure.

35. DCHL assures consumers, including Plaintiff(s) and Class Members, that “consumer privacy is important to us. We respect your right to privacy and will protect the information we maintain about you in the ongoing operation of the health benefit exchange (“Exchange”) in accordance with applicable laws, regulations and standards for security and privacy.”¹⁴ Plaintiff(s) and the Class Members, as consumers, relied on the promises and duties of DCHL to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

36. Consumers, in general, demand that businesses that require highly sensitive PII will provide security to safeguard their PII, especially when Social Security numbers are involved.

¹³ Privacy Policy, <https://dchealthlink.com/privacy> (last visited Mar. 14, 2023).

¹⁴ *Id.*

37. In the course of their dealings, including Plaintiff(s) and Class Members, provided DCHL with all or most of the following types of Private Information:

- First and last names;
- Home addresses;
- Dates of birth;
- Gender, race, ethnicity, and citizenship;
- Email addresses;
- Phone numbers;
- Social Security numbers.
- Financial information;
- Employment/employer information;
- Information relating to health insurance; and
- Photo identification and/or driver's licenses.

38. DCHL had a duty to adopt reasonable measures to protect Plaintiff(s)' and Class Members' PII from unauthorized disclosure to third parties. In addition, DCHL was aware of its duty to protect this PII.

The Data Breach

39. According to its Notice Letters, on March 6, 2023, DCHL "received notice that data for some DC Health Link customers had been exposed on a public forum." Its investigation determined that Plaintiff(s)' and Class Members' and their families' Private Information "was exposed."¹⁵

40. The Notice Letters are a tacit admission that an unauthorized actor—a cyber

¹⁵ See Exhibit A, Plaintiff's Notice Letter.

criminal—accessed DCHL’s network sometime before March 6, 2023 and was able to extract and publicly publish Plaintiff(s)’ and Class Members’ Private Information, undetected until the publication of that information was made known to DCHL.

41. Therefore, *Plaintiff(s)’ and Class Members’ PII was in the hands of cybercriminals for an undetermined amount of time before they were notified* of DCHL’s Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

42. DCHL admits that the files exfiltrated from DCHL contained at least the following information of Plaintiff(s) and Class Members: names, dependents’ names, addresses, Social Security numbers, email addresses, phone numbers, employer names and information, work emails, health care plans, race, and other highly sensitive information.¹⁶

43. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from DCHL that included the Private Information of Plaintiff(s) and Class Members.

44. Upon information and belief, the Private Information stored on DCHL’s network was not encrypted, despite a promise in its Privacy Notice that it would be (“We encrypt credit card numbers and other data that must remain secure to meet legal requirements.”).¹⁷

45. Plaintiff(s)’ Private Information was accessed and stolen in the Data Breach. Plaintiff(s) reasonably believe their stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information, and because DCHL’s Notice Letter alludes to the Private Information being “exposed” on a public forum.

¹⁶ *Id.*

¹⁷ <https://dchealthlink.com/privacy> (last accessed Mar. 14, 2023).

46. As a result of the Data Breach, DCHL now encourages Class Members to enroll in credit and identity monitoring and dark web monitoring, a tacit admission of the imminent risk of identity theft faced by Plaintiff(s) and Class Members as a direct result of its Data Breach.¹⁸

47. DCHL's encouragement for Plaintiff(s) and Class Members to enroll in these services is an acknowledgment that the impacted consumers are subject to a *substantial and imminent threat* of fraud and identity theft.

48. DCHL had obligations created by contract, industry standards, and common law to keep Plaintiff(s)'s and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

49. DCHL could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

Defendant Acquires, Collects, and Stores Plaintiff(s)'s and Class Members' PII

50. DCHL acquires, collects, and stores a massive amount of personally identifiable information ("PII") of consumers for whom it is providing health insurance services.

51. By obtaining, collecting, and using Plaintiff(s)' and Class Members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff(s)' and Class Members' PII from disclosure.

52. Plaintiff(s) and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

53. Plaintiff(s) and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach was a

¹⁸ Notice Letter, Exhibit A.

Foreseeable Risk of which Defendant was on Notice

54. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Business entities that collect such information, including DCHL, are well aware of the risk of being targeted by cybercriminals.

55. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

56. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, “[a] direct financial loss is the monetary amount the offender obtained from misusing the victim’s account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.”¹⁹

57. Individuals, like Plaintiff(s) and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person’s identity and is likened to accessing your DNA for hacker’s purposes.

58. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being

¹⁹ “Victims of Identity Theft, 2018,” U.S. Department of Justice (Apr. 2021, NCJ 256085) available at: <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed Mar.13, 2025).

misused, Plaintiff(s) and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

59. The Social Security Administration has warned that “a new number probably won’t solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won’t guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.”²⁰

60. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.²¹

61. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from “social engineering and ransomware” as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from “misconfigurations, human error, poor maintenance, and unknown assets.”²²

62. In light of high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its computer network would be targeted by

²⁰ <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Mar. 13, 2023).

²¹ <https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last accessed Mar. 13, 2023).

²² <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864> (last accessed Mar. 13, 2023).

cybercriminals.

63. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

64. According to an FBI publication, “[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.”²³ This publication also explains that “[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn’t guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.”²⁴

65. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, DCHL failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

66. Defendant failed to abide by its own Privacy Policy.²⁵

At All Relevant Times Defendant Had a Duty to Plaintiff(s) and Class Members to Properly Secure their Private Information

67. At all relevant times, DCHL had a duty to Plaintiff(s) and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff(s) and Class Members, and to promptly notify Plaintiff(s)

²³ <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware> (last accessed Mar. 13, 2023).

²⁴ *Id.*

²⁵ <https://dchealthlink.com/privacy> (last accessed on Mar. 13, 2023).

and Class Members when DCHL became aware that their PII was compromised.

68. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff(s) and Class Members.

69. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

- a. Maintaining a secure firewall configuration;
- b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- c. Monitoring for suspicious or irregular traffic to servers;
- d. Monitoring for suspicious credentials used to access servers;
- e. Monitoring for suspicious or irregular activity by known users;
- f. Monitoring for suspicious or unknown users;
- g. Monitoring for suspicious or irregular server requests;
- h. Monitoring for server requests for PII;
- i. Monitoring for server requests from VPNs; and
- j. Monitoring for server requests from Tor exit nodes.

70. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²⁶ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other

²⁶ 17 C.F.R. § 248.201 (2013).

things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”²⁷

71. The ramifications of Defendant’s failure to keep consumers’ PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver’s license numbers, fraudulent use of that information and damage to victims including Plaintiff(s) and the Class may continue for years.

The Value of Personal Identifiable Information

72. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200.²⁸

73. Criminals can also purchase access to entire company’s data breaches from \$900 to \$4,500.²⁹

74. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls

²⁷ *Id.*

²⁸ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Mar. 13, 2023).

²⁹ *In the Dark*, VPNOverview (2019), <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Mar. 13, 2023).

from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.³⁰

75. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

76. Even a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”³¹

77. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”³²

78. PII can be used to distinguish, identify, or trace an individual’s identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.³³

³⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Mar. 13, 2023).

³¹ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed Mar. 13, 2023).

³² Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Mar. 13, 2023).

³³ See [OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16](#) n.1 (last accessed Mar. 13, 2023).

79. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

80. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

81. Moreover, DCHL has offered only a limited three-year subscription for identity theft and dark web monitoring protection through Equifax, without any repayment for fraudulent charges made if the "monitoring" uncovers identity thefts. Its limitation is inadequate when DCHL's victims are likely to face many years of identity theft.

82. Furthermore, Defendant's credit monitoring offer and advice to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff(s) and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff(s) and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to protect themselves.

83. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff(s)' and Class Members' PII.

84. The injuries to Plaintiff(s) and Class Members were directly and proximately caused by DCHL's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

85. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission (“FTC”) has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.³⁴

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.³⁵ The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct security problems.

87. The FTC emphasizes that early notification to data breach victims reduces injuries: “If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused” and “thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim’s name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage.”³⁶

88. The FTC recommends that companies verify that third-party service providers have

³⁴ Federal Trade Commission, *Start With Security*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Mar. 13, 2023).

³⁵ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> (last accessed Mar. 13, 2023).

³⁶ <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> (last accessed Mar. 13, 2023).

implemented reasonable security measures.³⁷

89. The FTC recommends that businesses:

- a. Identify all connections to the computers where you store sensitive information.
- b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
- c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
- d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.
- f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.
- g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on

³⁷ See FTC, *Start With Security*, *supra*.

the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

- h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

90. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Because Class Members entrusted Defendant with their PII, Defendant had, and has, a duty to the Plaintiff(s) and Class Members to keep their PII secure.

92. Plaintiff(s) and the other Class Members reasonably expected that when they provide PII to DCHL, it would safeguard their PII.

93. DCHL was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff(s) and members of the Class. DCHL was also

aware of the significant repercussions if it failed to do so. Its own Privacy Policy, quoted above, acknowledges this awareness.

94. DCHL's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff(s)' and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff(s) and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

95. Plaintiff(s) and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

96. Defendant's poor data security deprived Plaintiff(s) and Class Members of the benefit of their bargain. Plaintiff(s) and other individuals whose PII was entrusted with DCHL understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff(s) and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff(s) and the Class Members suffered pecuniary injury.

97. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff(s) have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

98. The cybercriminals who obtained the Class Members' PII may exploit the

information they obtained by selling the data in so-called “dark markets” or on the “dark web.” Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member’s name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver’s license, birth certificate, or other public document.

99. In addition, if a Class Member’s Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person’s ability to gain employment or obtain a loan.

100. As a direct and/or proximate result of Defendant’s wrongful actions and/or inaction and the resulting Data Breach, Plaintiff(s) and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

101. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

102. Accordingly, Defendant’s wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff(s) and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, “[t]he level of risk is growing for anyone whose information is stolen in a data breach.” Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that “[t]he theft of SSNs places consumers

at a substantial risk of fraud.”³⁸ Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members’ PII will do so at a later date or re-sell it.

103. As a result of the Data Breach, Plaintiff(s) and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

104. DCHL admits that it learned “that data for some DC Health Link customers had been exposed on a public forum” , thereby acknowledging that it first learned of the Data Breach after cybercriminals actually exfiltrated Plaintiff(s)’ and Class Members’ PII.³⁹

***Data Breaches Put Consumers at an Increased Risk
Of Fraud and Identify Theft***

105. Data Breaches such as the one experienced Plaintiff(s) and Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

106. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.⁴⁰ Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers’ options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO’s recommendations that the steps Data Breach victims (like Plaintiff(s) and Class) must take after a breach like Defendant’s are both time consuming and of

³⁸ *The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas*, available at: https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf (last accessed Mar. 13, 2023).

³⁹ *See* Notice Letter, Ex. A.

⁴⁰ <https://www.gao.gov/assets/gao-19-230.pdf> (last accessed Jan. 19, 2023). *See* attached as Ex. B.

only limited and short-term effectiveness.

107. The GAO has long recognized that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record,” discussing the same in a 2007 report as well (“2007 GAO Report”).⁴¹

108. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁴²

109. Theft of Private Information is also gravely serious. PII is a valuable property right.⁴³

110. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

⁴¹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Gov. Accountability Office (June 2007), <https://www.gao.gov/new.items/d07737.pdf> (last accessed Mar. 14, 2023) (“2007 GAO Report”).

⁴² See <https://www.identitytheft.gov/Steps> (last accessed Mar. 14, 2023).

⁴³ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

See 2007 GAO Report, at p. 29.

111. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

112. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff(s) and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff(s) and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

Plaintiff Suhr’s Experience

113. Plaintiff Jenni Suhr is, and at all times relevant to this complaint, a resident and citizen of the State of Colorado.

114. Plaintiff Suhr is a consumer who applied for health insurance services through DCHL, in relation to her employer’s health insurance benefits. DCHL required that Plaintiff Suhr to provide it with her PII, including but not limited to her Social Security number.

115. On or about March 9, 2023, Plaintiff Suhr received an email directing her to check for a communication in her DC Health Link account. When she did, the Notice of Data Breach letter was in her file, informing her that her critical PII was “exposed on a public forum.”

116. The Notice letter stated that her exposed information included:

- a. Your name and name of your dependents enrolled on DC Health Link, Social Security Number, Date of Birth, Gender, Address, Email, and Phone Number. If your DC Health Link coverage is through an employer, then the employer name and information about the employer and work email.
- b. Additional information exposed included Plan name, Premium Amount, APTC, Coverage Start and End Dates, Race/Ethnicity, Citizenship, HBX ID.

See Suhr Notice of Data Breach Letter, attached as Exhibit A.

117. Plaintiff Suhr is alarmed by the amount of her Personal Information that was stolen or accessed, and even more by the fact that her Social Security number was identified as among the breach data on DCHL's computer system.

118. In response to DCHL's Notice of Data Breach, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, which will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

119. For a little over a month now, Plaintiff Suhr has been receiving a combination of around 5–6 spam calls, texts, and many spam emails per day. Prior to this time, she was receiving maybe one troublesome call and/or email per day. She reasonably believes these time consuming and annoying calls, text, and emails are related to DCHL's Data Breach given the timing of its awareness of the Data Breach.

120. Through DCHL's Notice Letter, Plaintiff Suhr was notified that her Private Information was "publicly exposed" which she assumes means that it has been found on the dark web.

121. Plaintiff has obtained the credit monitoring service offered by DCHL but believes that it is inadequate, since her Private Information is likely to be abused and sold repeatedly for a matter of many years. The service will not reimburse her for her time and expenses associated with identity fraud and theft.

122. Immediately after receiving the Notice Letter, Plaintiff spent time discussing her options and has started to check her financial accounts for a minimum of thirty minutes per day in an effort to mitigate the damage that has been caused by DCHL.

123. Plaintiff is very careful about sharing PII and has never knowingly transmitted

unencrypted PII over the internet or any other unsecured source.

124. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided DCHL with her PII had DCHL disclosed that it lacked data security practices adequate to safeguard PII.

125. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that she entrusted to DCHL.

126. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

127. Plaintiff Suhr reasonably believes that her Private Information has already been sold by the cybercriminals. Had she been notified of DCHL's breach before the Private Information was posted on a public forum, she could have attempted to mitigate her injuries.

128. Plaintiff Suhr has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third-party criminals.

129. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief remains backed up and in DCHL's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

130. Plaintiff(s) brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

131. Plaintiff(s) proposes the following Class definition, subject to amendment as appropriate:

All individuals whose Private Information was maintained on DC Health Link's computer systems and who were sent a notice of DCHL's 2023 Data Breach.

132. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

133. Plaintiff(s) hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

134. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff(s) at this time, based on information and belief, the Class consists between 56,000 and 170,000 persons whose data was compromised in Data Breach.

135. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff(s)' and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff(s) and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- l. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

136. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff(s)' Private Information, like that of every other Class Member, was compromised in the Data Breach.

137. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel are competent and experienced in litigating Class actions.

138. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common

issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

139. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

140. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

141. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

142. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by DCHL.

CAUSES OF ACTION

FIRST COUNT

Negligence

(On behalf of Plaintiff(s) and All Class Members)

143. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

144. Defendant gathered and stored the Private Information of Plaintiff(s) and Class Members as part of the regular course of its business operations. Plaintiff(s) and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

145. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's

duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

146. Defendant owed a duty of care to Plaintiff(s) and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

147. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits “unfair ... practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

148. Plaintiff(s) and the Class are within the class of persons that the FTC Act was intended to protect.

149. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff(s) and the Class.

150. Defendant gathered and stored the Private Information of Plaintiff(s) and Class Members as part of its business of soliciting its services to its clients and its clients’ patients, which solicitations and services affect commerce.

151. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff(s) and Class Members and by not complying with applicable industry standards, as described herein.

152. Defendant breached its duties to Plaintiff(s) and Class Members under the FTC Act

by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff(s)' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

153. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who received its services, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

154. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

155. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

156. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff(s) and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

157. Plaintiff(s) and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff(s) and the Class Members had no ability to protect their Private Information that was in Defendant's possession.

158. Defendant was in a special relationship with Plaintiff(s) and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiff(s) and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiff(s)' and Class Members' Private Information. The harm to Plaintiff(s)

and Class Members from its exposure was highly foreseeable to Defendant.

159. Defendant owed Plaintiff(s) and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff(s) and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff(s) and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

160. Defendant's duty extended to protecting Plaintiff(s) and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

161. Defendant had duties to protect and safeguard the Private Information of Plaintiff(s) and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff(s) and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff(s)' and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;
- b. To protect Plaintiff(s)' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and
- c. To promptly notify Plaintiff(s) and Class Members of any breach, security

incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

162. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

163. Defendant breached its duties of care by failing to adequately protect Plaintiff(s)' and Class Members' Private Information. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;
- b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;
- c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;
- d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;
- e. Failing to consistently enforce security policies aimed at protecting Plaintiff(s)' and Class Members' Private Information;
- f. Failing to mitigate the harm caused to Plaintiff(s) and the Class Members;
- g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and
- h. Failing to promptly notify Plaintiff(s) and Class Members of the Data Breach that affected their Private Information.

164. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

165. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff(s) and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

166. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff(s) and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff(s) and Class Members while it was within Defendant's possession and control.

167. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff(s) and Class Members, Defendant prevented Plaintiff(s) and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

168. As a result of the Data Breach, Plaintiff(s) and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

169. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

170. The damages Plaintiff(s) and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

171. Plaintiff(s) and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiff(s) and All Class Members)

172. Plaintiff(s) re-allege and incorporate by the paragraphs above as if fully set forth herein.

173. Plaintiff(s) and Class Members were required to provide their PII to Defendant as a condition of receiving insurance services provided by Defendant.

174. Plaintiff(s) and Class Members provided their PII to Defendant in exchange for DCHL's services. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

175. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiff(s) and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

176. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff(s)'s and Class Members' Private Information would remain protected.

177. Implicit in the agreement between Plaintiff(s) and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff(s) and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff(s) and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

178. When Plaintiff(s) and Class Members provided their Private Information to

Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

179. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

180. In entering into such implied contracts, Plaintiff(s) and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

181. Plaintiff(s) and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff(s) and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

182. Plaintiff(s) and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

183. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

184. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

185. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

186. Plaintiff(s) and Class Members are also entitled to nominal damages for the breach of implied contract.

187. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff(s) and All Class Members)

188. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

189. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

190. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff(s) and Class Members and accepted that monetary benefit.

191. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff(s)' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff(s) and Class Members by utilizing cheaper, ineffective security measures. Plaintiff(s) and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

192. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff(s) and Class Members, because Defendant failed to implement appropriate data management and security measures.

193. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

194. If Plaintiff(s) and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

195. Plaintiff(s) and Class Members have no adequate remedy at law.

196. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

197. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

198. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff(s) and Class Members, proceeds that they unjustly received from them.

FOURTH COUNT
Declaratory Judgment
(On Behalf of Plaintiff(s) and All Class Members)

199. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

200. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

201. An actual controversy has arisen in the wake of the DCHL Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether DCHL is currently maintaining data security measures adequate to protect Plaintiff(s) and Class Members from further data breaches that compromise their Private Information.

202. Plaintiff(s) allege that DCHL's data security measures remain inadequate. Plaintiff(s) will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

203. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. DCHL continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, and Section 5 of the FTC Act;
- b. DCHL continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

204. The Court also should issue corresponding prospective injunctive relief requiring DCHL to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

205. If an injunction is not issued, Plaintiff(s) and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at DCHL. The risk of another such breach is real, immediate, and substantial. If another breach at DCHL occurs, Plaintiff(s) and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

206. The hardship to Plaintiff(s) and Class Members if an injunction does not issue exceeds the hardship to DCHL if an injunction is issued. Among other things, if another massive data breach occurs at DCHL, Plaintiff(s) and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to DCHL of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and DCHL has a pre-existing legal obligation to employ such measures.

207. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at DCHL, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff(s) and their counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiff(s)' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff(s) and Class Members;

- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- E. For declaratory relief as requested;
- F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff(s) and the Class;
- G. For an award of actual damages, compensatory damages, and statutory damages, in an amount to be determined, as allowable by law;
- H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- I. Pre- and post-judgment interest on any amounts awarded; and
- J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff(s) demand a trial by jury on all claims so triable.

Dated: March 15, 2023

Respectfully submitted,

/s/ Gary E. Mason

Gary E. Mason (DC Bar 418073)

Danielle L. Perry (DC Bar 1034960)

MASON LLP

5335 Wisconsin Avenue NW, Suite 640

Washington, DC 20015

Tel: (202) 429-2290

Email: gmason@masonllp.com

Email: dperry@masonllp.com

Attorneys for Plaintiff(s)

EXHIBIT A

DC Health Link
1225 I Street, NW
Suite 400
Washington, DC 20005



RE: NOTICE OF DATA BREACH

We are contacting you about a data breach involving your personally identifiable information (PII).

WHAT HAPPENED

On March 6, 2023, we received notice that data for some DC Health Link customers had been exposed on a public forum. We immediately initiated a comprehensive investigation and are working with forensic investigators and law enforcement. The investigation is ongoing and we will provide more information as we have more to share.

You are receiving this letter because we have determined that your information and information of your family members in your DC Health Link account was exposed.

We are providing credit and identity monitoring protection services that you can access immediately, at no cost to you.

WHAT INFORMATION WAS INVOLVED IN THE DATA BREACH

The personally identifiable information that was exposed included the following:

- Your name and name of your dependents enrolled on DC Health Link, Social Security Number, Date of Birth, Gender, Address, Email, and Phone Number. If your DC Health Link coverage is through an employer, then the employer name and information about the employer and work email.
- Additional information exposed included Plan name, Premium Amount, APTC, Coverage Start and End Dates, Race/Ethnicity, Citizenship, HBX ID

WHAT WE ARE DOING

In addition to immediately initiating a comprehensive investigation and working with forensic investigators and law enforcement, we contracted with Experian to provide the following to DC Health Link customers whose personally identifiable information was exposed:

- 3 years of credit and identity monitoring protection, including tracking through all three credit bureaus and dark web identity monitoring.
- To activate this protection, you must enroll using the codes provided below.

We will also be providing these services to all DC Health Link customers (including those not directly affected by the incident) out of an abundance of caution.

WHAT YOU CAN DO

You can sign up immediately for monitoring services through Experian using the following codes. We encourage you to enroll yourself, as well as all family members and dependents on your account.

Visit the Experian IdentityWorks website to enroll:

- For adult DC Health Link customers (18 and over), go to <https://www.experianidworks.com/3bplus>

- Activation Code: [REDACTED]
 - Engagement Number: [REDACTED]
 - Product: Experian IdentityWorks – Credit Plus 3B
-
- For DC Health Link customers who are minors (under 18), go to <https://www.experianidworks.com/minorplus>
 - Activation Code: [REDACTED]
 - Engagement Number: [REDACTED]
 - Product: Experian IdentityWorks – Minor Plus

You will need to provide the **Activation Code** listed above for the adult or minor monitoring services you are selecting.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian’s customer care team at **(877) 890-9332**. Be prepared to provide the **Engagement Number** listed for your services above as proof of eligibility for the identity restoration services by Experian. If asked for a “Client Name” mention **District of Columbia Health Benefit Exchange Authority**.

You can visit FTC’s website, [IdentityTheft.gov/databreach](https://www.ftc.gov/identitytheft), about steps you can take to help protect yourself from identity theft.

FOR MORE INFORMATION

For all other questions, you may call DC Health Link at (855) 532-5465 (TTY: 711).

Sincerely,
DC Health Link



Get help in your language

This Notice has Important Information. This notice has important information about your application or coverage through DC Health Link. Look for key dates in this notice. You may need to take action by certain deadlines to keep your health coverage or help with costs. You have the right to get this information and help in your language at no cost. Call (855) 532-5465.

Este aviso contiene información importante. Este aviso contiene información importante acerca de su solicitud o su seguro con DC Health Link. Preste atención a las fechas que aparecen en este aviso, puesto que podría ser necesaria alguna acción por su parte antes de determinada fecha a fin de mantener su seguro médico con nosotros o sus ayudas con el coste. Usted tiene derecho a recibir esta información y soporte en su idioma sin coste adicional. Llame al (855) 532-5465.

ይህ ማስታወቂያ አስፈላጊ መረጃ ይዟል። ይህ ማስታወቂያ ስለ ማመልከቻዎ ወይም ስለ DC Health Link ሽፋን አስፈላጊ መረጃ አለው። በዚህ ማስታወቂያ ውስጥ ቁልፍ ቀንችን ፈልጉ። የጤና ሽፋንዎን ለመጠበቅ እና በአካፋፈሉ እርዳታ ለማግኘት በተወሰኑ የጊዜ ገደቦች እርምጃ መውሰድ ይገባዎት ይሆናል። ይህን መረጃ ለማግኘት እና ያለ ምንም ክፍያ በቋንቋዎ እርዳታ የማግኘት መብት አልዎት። በ (855) 532-5465 ላይ ይደውሉ።

本通知包含重要信息。本通知包含有关您通过 DC Health Link 提交申请和保险的重要信息。请查看本通知中的关键日期。您可能需要在特定截止日期前采取行动，以便维持您的健康保险或有助于降低费用。您有权免费以自己的母语获得本信息和帮助。请致电 (855) 532-5465。

Cet avis contient des informations importantes. Cet avis contient des informations importantes au sujet de votre demande ou de la couverture par DC Health Link. Cherchez les dates clés dans cet avis. Vous devrez peut-être prendre des mesures en respectant certaines échéances afin de maintenir votre couverture de santé ou d'assumer des coûts. Vous avez le droit d'obtenir ces informations et d'être aidé dans votre langue sans frais. Appelez le (855) 532-5465.

May Importanteng Impormasyon ang abisong ito. May Importanteng Impormasyon ang abisong ito tungkol sa aplikasyon mo o proteksiyon mo sa DC Health Link. Tingnan ang mga importanteng petsa na nasa abisong ito. Maaaring may mga kailangan kang gawin bago sumapit ang ilang deadline para mapanatili ang proteksiyon mo sa kalusugan o para makatulong sa mga gastusin. Karapatan mong makuha ang impormasyon na ito at makakuha ng tulong na nasa wika mo nang walang gastos. Tumawag sa (855) 532-5465.

В настоящем уведомлении содержится важная информация. В этом уведомлении содержится важная информация о вашем заявлении или страховом покрытии посредством DC Health Link. Посмотрите на ключевые даты в настоящем уведомлении. Вам, возможно, потребуются принять меры к определенным предельным срокам для сохранения страхового покрытия или помощи с расходами. Вы имеете право на бесплатное получение этой информации и помощи на вашем языке. Звоните по телефону (855) 532-5465.

Este aviso contém informações importantes. Este aviso contém informações importantes sobre o seu pedido ou cobertura através da DC Health Link. Procure as datas chave neste aviso. Poderá necessitar de tomar providências dentro de certos prazos para manter a sua cobertura de saúde ou para obter ajuda com custos. Tem o direito de obter estas informações e ajuda no seu idioma sem qualquer custo. Ligue (855) 532-5465.

Questo avviso contiene informazioni importanti. Questo avviso contiene informazioni importanti sulla tua domanda o copertura attraverso DC Health Link. Cerca le date chiave in

questo avviso.

Potrebbe essere necessario un tuo intervento entro una scadenza determinata per consentirti di mantenere la tua copertura o una sovvenzione. Hai il diritto di ottenere queste informazioni e assistenza nella tua lingua gratuitamente. Chiama (855) 532-5465.

Thông báo này có Thông tin Quan trọng. Thông báo này có thông tin quan trọng về đơn hoặc hợp đồng bảo hiểm của bạn qua DC Health Link. Xin xem những ngày quan trọng trong thông báo này. Quý vị có thể phải thực hiện theo đúng thời hạn để duy trì bảo hiểm sức khỏe hoặc giúp đỡ chi phí. Quý vị có quyền được biết thông tin này và được trợ giúp bằng ngôn ngữ của mình miễn phí. Xin gọi số (855) 532-5465.

Libihne lini li gwe banga bi niigana. Libihne lini li gwe banga bi niigana kolbaha ni ndjombi yor tole ma teeda mor lor ni DC Health Link. Yer ma kel ma tobo tobo munu libihne lini. Bebeg le u ga bana nguim mam i bor nwaa le guim di loo di kola i nyu I teda mateda tole nsaa u mboo wor. U gwee kundi kosna biniguene bini ni mahola ni hop wong ngui nsaa wogui wo. Sebel I nsinga ini (855) 532-5465.

Ihe Nkwupụta a were ozi di mkpa banyere ya. Ihe Nkwupụta a were ozi di mkpa banyere ya gbasara maka arịrịọ gị ma obu ọgwụgwọ site na DC Health Link. Lee anya maka ụbọchị dị-karịrị mkpa na ihe nkwupụta a. I were ike jchọ ime ihe na ụfọdụ oge mgwucha ka idebe ọgwụgwọ ahụ ike gị ma obu enyemaka na ikwu ụgwọ. Inwere ikike inweta ozi a na enyemaka na asụsụ gị n'efu. Kpoo (855) 532-5465.

Àkíyèsí yíí ní Ifitonilétí Pàtàkì Nínú. Àkíyèsí yíí ní ifitonilétí pàtàkì nípá lẹ̀ta-isèbèèrè tàbí idójútòfò rẹ̀ nípá DC Health Link nínú. Se àwàrí àwọn ojú pàtàkì tí n bẹ̀ nínú àkíyèsí yíí. O lẹ̀ ní láti gbe àwọn igbèsẹ̀ ní ìbámu pẹ̀lú àwọn ojú tó gbẹ̀yìn kan ní pàtò láti lẹ̀ pa idójútòfò ilera rẹ̀ tàbí iseranwọ̀ fun ọ̀ mọ̀ pẹ̀lú sísanwọ̀. O ní ẹ̀tọ̀ lati rí iranwọ̀ àti ifitonilétí yíí gbà ní èdè rẹ̀ láìsanwọ̀. Pẹ̀ sórí (855) 532- 5465.

এই ইনোভেশনেট পূর্ণ তথ্য আছে। DC Health Link এর মাধ্যমে আপনার আবেদন পূর্ণ বা কভারের জন্য
সহযোগিতা

এই নোংরা পুণ তথ্যে। মূল তারিখের জন এই নোংরা টেদেখুন। কিছু নিদিষ্ট সময়সীমা অনুসারে

আপনার **৭০%** কভারেজ বা তার মূলে~~৭০%~~র ~~০০%~~ আপনার **০কান কম৭০%** যা **৭**হণ করার **৭**য়োজন হৈত পারে।

আপনার এই তথ্যটি বিনামূল্যে আপনার ভাষায় পাওয়ার অধিকার আছে। (855) 532-5465 নম্বরের কল করুন।

この通知には重要な情報が含まれています。この通知には DC Health Link の申請または補償範囲に関する重要な情報が含まれています。この通知に記載されている重要な日付をご確認ください。健康保険や有料サポートを維持するには、特定の期日までに行動を取らなければならない場合があります。ご希望の言語による情報とサポートが無料で提供されます。(855) 532-5465 までお電話ください。

본 통지서는 중요한 정보를 포함하고 있습니다. 이 통지서는 DC Health Link 관련 귀하 또는 귀하의 보험 적용 대상자에 대한 정보가 들어 있습니다. 이 통지서에 나와 있는 중요 날짜를 참조하시기 바랍니다. 건강 보험을 유지하거나 보험료 지원을 받으시려면 해당 만료일자까지 연장하시기 바랍니다. 이에 대한 정보를 귀하의 언어로 비용 부담없이 지원을 받으실 수 있습니다. 해당 언어의 통역사에게 문의하시려면 (855) 532-5465로 전화하십시오.

ใบประกาศนียบัตร ใบประกาศนียบัตร อัญมณีศาสตร์ เกี่ยวกับ การสมัครหรือ ขอบเขตประกัน สุขภาพของคุณกับ DC

Health Link โปรดดูกำหนดการในใบประกาศนี้ หัด
คุณอาจจะขอ ดาเนินการภายในกำหนดระยะเวลาที่ นอนแพ้อี หี ร์ก ษาการประนสุขภาพของคุณหรือ การขอรองความช่วยเหลือ
อีกคำใช้จ่า ย คุณมสทหี ะได้รับข้อ มูลและความช่วยเหลือเกี่ วกับเรี ่งนี้ นหาษาของคุณโดยไม่ต้องเสียอะไร โทร (855)
532- 5465

Die Nachricht enthält wichtige Informationen bezüglich Ihres Antrags bei oder Ihres Versicherungsschutzes durch DC Health Link. Suchen Sie nach Schlüsselwörtern in dieser Nachricht. Sie müssen eventuell vor einer bestimmten Frist reagieren, um Ihren Versicherungsschutz aufrechtzuerhalten oder um Hilfe bezüglich der Kosten zu erhalten. Sie haben das Recht, diese Information und Hilfe kostenfrei in Ihrer Sprache zu erhalten. Wählen Sie hierfür (855) 532-5465.

يحتوي هذا الإشعار معلومات هامة. يحتوي هذا الإشعار معلومات هامة بخصوص طلبك أو تغطيتك من خلال DC Health Link. ابحث عن التواريخ الهامة في هذا الإشعار. قد تحتاج لاتخاذ اجراء في تواريخ معينة للحفاظ على تغطيتك الصحية او للمساعدة في دفع التكاليف. لك الحق في الحصول على هذه المعلومات والمساعدة بلغتك من دون أي تكلفة. اتصل بـ-(855) 532-5465.

The D.C. Health Benefit Exchange Authority (DC HBX) complies with applicable Federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, or sex. This agency does not exclude people or treat them differently because of race, color, national origin, age, disability, or sex.

DC HBX:

- Provides free support and services to people with disabilities to communicate effectively with us, such as:
 - Qualified sign language interpreters
 - Written information in other formats (large print, audio, accessible electronic formats, other formats)
- Provides free language services to people whose primary language is not English, such as:
 - Qualified interpreters
 - Information written in other languages

If you need these services, contact:

DC Health Link Contact Center
Phone: (855) 532-5465
TTY: 711
Email: info@dchealthlink.com

If you believe that the D.C. Health Benefit Exchange Authority has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance in person or by mail, fax, or email. with: Jennifer Libster, Associate General Counsel, D.C. Health Benefit Exchange Authority, 1225 Eye Street NW, Suite 400, Washington DC 20005, (202) 715-7576, TTY: 711, 1557.grievance@dc.gov; Fax: (202) 730-1658. You must file a grievance within 60 days of the date you became aware of the alleged discriminatory action. Jennifer Libster is also available to help you with the grievance filing process.

You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights electronically through the Office for Civil Rights Complaint Portal, available at <https://ocrportal.hhs.gov/ocr/portal/lobby.jsf>, or by mail or phone at:

U.S. Department of Health and Human Services,
200 Independence Avenue SW.,
Room 509F, HHH Building,
Washington, DC 20201
1-800-868-1019, 1-800-537-7697 (TDD).

Complaint forms are available at <http://www.hhs.gov/ocr/office/file/index.html>.

EXHIBIT B




Appendix II: What Can Consumers Do After a Data Breach?

Figure 3 below provides information on actions consumers can take to monitor for identity theft or other forms of fraud, protect their personal information, and respond if they have been a victim of identity theft. This information summarizes prior GAO work and comments of academic, consumer organization, industry, and government experts.¹

¹GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, [GAO-17-254](#) (Washington, D.C.: Mar. 30, 2017).

Appendix II: What Can Consumers Do After a Data Breach?

Figure 3: What Can Consumers Do After a Data Breach?




Prevent Fraud on New Credit Accounts			
Consumer Option	How This Option Can Help	Consumers Should Be Aware	
 <p>Place a credit freeze on credit reports at Equifax, Experian, and TransUnion—the three nationwide consumer reporting agencies.</p>	<ul style="list-style-type: none">• Prevents identity thieves from opening new credit accounts in an individual’s name—where credit reports are required.• Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated.	<ul style="list-style-type: none">• Consumers must request a freeze at each of the three agencies separately.• Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports.• Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card).• Freezes do not prevent other types of harm, such as tax refund or medical identity fraud.• Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks).• Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts).	
 <p>Fraud Alert</p>	<p>Place a fraud alert at the three nationwide consumer reporting agencies, which lasts 1 year and can be renewed.</p> <ul style="list-style-type: none">• Fraud alerts let businesses know that a consumer may have been a victim of fraud.• Businesses must take extra steps to verify the identity of the individual seeking to open accounts.• Members of the military can place active duty alerts.	<ul style="list-style-type: none">• Consumers can request a fraud alert at one of the three agencies and this agency must notify the other two to place the alert.• Victims of identity theft can place extended fraud alerts that last for 7 years.• Fraud alerts still allow access to credit reports.• Businesses that do not use the three agencies will not see the alert.	

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Appendix II: What Can Consumers Do After a Data Breach?

Monitor for Some Types of Fraud on Financial Accounts



Consumer Option	How This Option Can Help	Consumers Should Be Aware
 <p>Review free credit reports every 12 months (from Equifax, Experian, and TransUnion) at annualcreditreport.com.</p>	<ul style="list-style-type: none"> Can help consumers spot suspicious activity or fraud involving credit accounts. 	<ul style="list-style-type: none"> Consumers can check one of the three reports every 4 months to improve chances of catching problems throughout the year.
 <p>Review bank and other financial account statements regularly or set up free automatic alerts.</p>	<ul style="list-style-type: none"> Can alert consumers to suspicious activity on their accounts. 	<ul style="list-style-type: none"> The availability and features of alerts may vary among financial institutions.
 <p>Consider enrolling in credit or identity monitoring services.</p>	<ul style="list-style-type: none"> Credit monitoring can alert consumers after the fact that someone may have used their personal information to open a credit account (take out a loan or sign up for a credit card). Identity monitoring can alert consumers of misuse of personal information or appearance of their information on illicit websites (the “dark web”). 	<ul style="list-style-type: none"> These services do not directly address risks of medical identity theft, identity theft tax refund fraud, or government benefits fraud. Credit monitoring can spot fraud but generally cannot prevent it, and does not identify fraud on existing or noncredit accounts. Identity monitoring also cannot prevent fraud. It is unclear what actions consumers can take once alerted that their information appears on the dark web other than continuing to monitor their accounts. These services may be part of a package of identity theft services, including restoration services, or identity theft insurance. Free services that entities that have experienced data breaches may offer to affected consumers vary in the type and level of service and may only last for 1-2 years. Risks can exist for much longer. Paid services typically cost \$5–\$30 a month.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Appendix II: What Can Consumers Do After a Data Breach?

Monitor for Other Types of Identity Theft or Fraud



Consumer Option

How This Option Can Help

Consumers Should Be Aware



Mobile Phone or Utility Account Fraud

Review mobile phone and utility bills regularly.

- Can spot suspicious activity on existing accounts.
- Consumers with credit freezes may need to lift them before applying for new utility or phone accounts.



Medical Identity Theft

Review medical bills and health insurance explanations of benefits.

- Can spot suspicious activity, such as bills or insurance claims for services consumers did not receive.
- Consumers who spot problems can contact fraud departments at health insurers.



Identity Theft Tax Refund Fraud

File tax returns early.

- Provides less time for a fraudster to file in an individual's name.
- Consumers who experience identity theft tax refund fraud can file affidavits with the Internal Revenue Service (IRS) and through IdentityTheft.gov, and may be eligible to obtain an Identity Protection Personal Identification Number from IRS.



Government Benefits Fraud

Set up an online account at the Social Security Administration and check it regularly.




- Can spot suspicious activity, such as benefits redirected to another address.
- Other government benefits, such as unemployment insurance, also can be susceptible to identity fraud.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Appendix II: What Can Consumers Do After a Data Breach?

How to Respond after Identity Theft



Consumer Option	How This Option Can Help	Consumers Should Be Aware
 <p>Visit identityTheft.gov to set up an account, fill out, and file necessary reports.</p>	<ul style="list-style-type: none"> Helps users determine what steps to take depending on the type of information stolen or type of identity theft. Can generate an Identity Theft Report that can be used to help contact consumer reporting agencies, law enforcement, and other entities. Can generate an IRS Identity Theft Affidavit (IRS Form 14039) that can be submitted directly to IRS. Provides information on what companies to contact and how to remove incorrect information. 	<ul style="list-style-type: none"> The Federal Trade Commission (FTC) also has a telephone help line and online chat feature.
 <p>Contact state or local government resources, such as consumer protection help lines or victim services offices.</p>	<ul style="list-style-type: none"> Some states and local governments can provide one-on-one assistance. 	<ul style="list-style-type: none"> States and localities vary in the services offered.
 <p>Consider using commercial identity restoration services.</p>	<ul style="list-style-type: none"> Can reduce consumer time and effort in dealing with the effects of identity theft, such as by interacting with creditors on the consumer's behalf. 	<ul style="list-style-type: none"> Service levels can vary significantly among companies. Some provide hands-on assistance, while others largely provide information. May be included in a package of identity theft services, which may also include credit or identity monitoring or identity theft insurance. Paid services typically cost \$5–\$30 a month and free services may only be offered for 1-2 years.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Appendix II: What Can Consumers Do After a Data Breach?

Protect Personal Information in Other Ways



Consumer Option

How This Option Can Help

Consumers Should Be Aware



Adopt Good Practices for Online Accounts

- Protect passwords and do not re-use them.
- Use two-factor authentication when offered (for example, entering a one-time code sent to a mobile phone when logging in to an online account).
- Choose strong passwords and consider using a software application that helps manage passwords.
- Do not click on links in emails or open attachments from unknown senders.
- Remember that public WiFi may not be secure.

- Can prevent unauthorized access to online accounts and other data intrusions.

- While personal security practices are important, consumers have limited control over how private entities secure their data.



Protect social media accounts by checking privacy settings, and consider limiting information shared.

- Restricts how much information is visible to strangers and their ability to misuse it.

- Privacy terms and conditions can change, so it is important to check settings periodically.



Do not provide personal information over the phone (or by email or text) unless you've initiated the call (or communication).

- Prevents identity thieves from obtaining information that can be used to commit fraud.

- Consumers can do online searches to verify identities of requesters, or check with experts, before giving out information.
- Consumers should not trust caller ID and should hang up on robocalls and report such calls to FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).



Shred documents and mail with Social Security numbers or other personal information.

- Prevents identity thieves from finding sensitive information in trash.

- Consumers can contact the U.S. Postal Service if they believe their mail is being stolen or misdirected.
- Consumers can opt out of receiving credit card and other offers in the mail at 1-888-5-OPT-OUT (1-888-567-8688) or www.optoutprescreen.com.

CIVIL COVER SHEET

JS-44 (Rev. 11/2020 DC)

I. (a) PLAINTIFFS Jenni Suhr (b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF <u>Arapahoe</u> (EXCEPT IN U.S. PLAINTIFF CASES)	DEFENDANTS District of Columbia Health Benefit Exchange Authority, d/b/a DC Health Link COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____ (IN U.S. PLAINTIFF CASES ONLY) <small>NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED</small>
(c) ATTORNEYS (FIRMNAME, ADDRESS, AND TELEPHONE NUMBER) MASON LLP 5335 Wisconsin Ave., NW, Ste. 640, Washington, DC 20015; (202) 429-2290	ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION (PLACE AN x IN ONE BOX ONLY)	III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN x IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT) FOR DIVERSITY CASES ONLY!																								
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <input type="radio"/> 1 U.S. Government Plaintiff </div> <div style="width: 48%;"> <input type="radio"/> 3 Federal Question (U.S. Government Not a Party) </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 48%;"> <input type="radio"/> 2 U.S. Government Defendant </div> <div style="width: 48%;"> <input checked="" type="radio"/> 4 Diversity (Indicate Citizenship of Parties in item III) </div> </div>	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th style="text-align: center;">PTF</th> <th style="text-align: center;">DFT</th> <th></th> <th style="text-align: center;">PTF</th> <th style="text-align: center;">DFT</th> </tr> </thead> <tbody> <tr> <td>Citizen of this State</td> <td style="text-align: center;"><input type="radio"/> 1</td> <td style="text-align: center;"><input type="radio"/> 1</td> <td>Incorporated or Principal Place of Business in This State</td> <td style="text-align: center;"><input type="radio"/> 4</td> <td style="text-align: center;"><input checked="" type="radio"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td style="text-align: center;"><input checked="" type="radio"/> 2</td> <td style="text-align: center;"><input type="radio"/> 2</td> <td>Incorporated and Principal Place of Business in Another State</td> <td style="text-align: center;"><input type="radio"/> 5</td> <td style="text-align: center;"><input type="radio"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td style="text-align: center;"><input type="radio"/> 3</td> <td style="text-align: center;"><input type="radio"/> 3</td> <td>Foreign Nation</td> <td style="text-align: center;"><input type="radio"/> 6</td> <td style="text-align: center;"><input type="radio"/> 6</td> </tr> </tbody> </table>		PTF	DFT		PTF	DFT	Citizen of this State	<input type="radio"/> 1	<input type="radio"/> 1	Incorporated or Principal Place of Business in This State	<input type="radio"/> 4	<input checked="" type="radio"/> 4	Citizen of Another State	<input checked="" type="radio"/> 2	<input type="radio"/> 2	Incorporated and Principal Place of Business in Another State	<input type="radio"/> 5	<input type="radio"/> 5	Citizen or Subject of a Foreign Country	<input type="radio"/> 3	<input type="radio"/> 3	Foreign Nation	<input type="radio"/> 6	<input type="radio"/> 6
	PTF	DFT		PTF	DFT																				
Citizen of this State	<input type="radio"/> 1	<input type="radio"/> 1	Incorporated or Principal Place of Business in This State	<input type="radio"/> 4	<input checked="" type="radio"/> 4																				
Citizen of Another State	<input checked="" type="radio"/> 2	<input type="radio"/> 2	Incorporated and Principal Place of Business in Another State	<input type="radio"/> 5	<input type="radio"/> 5																				
Citizen or Subject of a Foreign Country	<input type="radio"/> 3	<input type="radio"/> 3	Foreign Nation	<input type="radio"/> 6	<input type="radio"/> 6																				

IV. CASE ASSIGNMENT AND NATURE OF SUIT

(Place an X in one category, A-N, that best represents your Cause of Action and one in a corresponding Nature of Suit)

<input type="radio"/> A. Antitrust <input type="checkbox"/> 410 Antitrust	<input type="radio"/> B. Personal Injury/Malpractice <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Medical Malpractice <input type="checkbox"/> 365 Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Product Liability	<input type="radio"/> C. Administrative Agency Review <input type="checkbox"/> 151 Medicare Act <u>Social Security</u> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <u>Other Statutes</u> <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 890 Other Statutory Actions (If Administrative Agency is Involved)	<input type="radio"/> D. Temporary Restraining Order/Preliminary Injunction Any nature of suit from any category may be selected for this category of case assignment. *(If Antitrust, then A governs)*
---	--	--	--

<input type="radio"/> E. General Civil (Other)	<input type="radio"/> F. Pro Se General Civil
---	--

<u>Real Property</u> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent, Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property <u>Personal Property</u> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<u>Bankruptcy</u> <input type="checkbox"/> 422 Appeal 27 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <u>Prisoner Petitions</u> <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Conditions <input type="checkbox"/> 560 Civil Detainee – Conditions of Confinement <u>Property Rights</u> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent – Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 (DTSA)	<u>Federal Tax Suits</u> <input type="checkbox"/> 870 Taxes (US plaintiff or defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609 <u>Forfeiture/Penalty</u> <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other <u>Other Statutes</u> <input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 430 Banks & Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 462 Naturalization Application	<input type="checkbox"/> 465 Other Immigration Actions <input type="checkbox"/> 470 Racketeer Influenced & Corrupt Organization <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act (TCPA) <input type="checkbox"/> 490 Cable/Satellite TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes <input type="checkbox"/> 890 Other Statutory Actions (if not administrative agency review or Privacy Act)
---	---	--	--

<input type="radio"/> G. Habeas Corpus/ 2255 <input type="checkbox"/> 530 Habeas Corpus – General <input type="checkbox"/> 510 Motion/Vacate Sentence <input type="checkbox"/> 463 Habeas Corpus – Alien Detainee	<input type="radio"/> H. Employment Discrimination <input type="checkbox"/> 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation) *(If pro se, select this deck)*	<input type="radio"/> I. FOIA/Privacy Act <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 890 Other Statutory Actions (if Privacy Act) *(If pro se, select this deck)*	<input type="radio"/> J. Student Loan <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (excluding veterans)
<input type="radio"/> K. Labor/ERISA (non-employment) <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 740 Labor Railway Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act	<input type="radio"/> L. Other Civil Rights (non-employment) <input type="checkbox"/> 441 Voting (if not Voting Rights Act) <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 445 Americans w/Disabilities – Employment <input type="checkbox"/> 446 Americans w/Disabilities – Other <input type="checkbox"/> 448 Education	<input checked="" type="radio"/> M. Contract <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholder's Suits <input checked="" type="checkbox"/> 190 Other Contracts <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<input type="radio"/> N. Three-Judge Court <input type="checkbox"/> 441 Civil Rights – Voting (if Voting Rights Act)

V. ORIGIN
☒ 1 Original Proceeding
 ☐ 2 Removed from State Court
 ☐ 3 Remanded from Appellate Court
 ☐ 4 Reinstated or Reopened
 ☐ 5 Transferred from another district (specify)
 ☐ 6 Multi-district Litigation
 ☐ 7 Appeal to District Judge from Mag. Judge
 ☐ 8 Multi-district Litigation – Direct File

VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)
 28 U.S.C. Section 1332(d)

VII. REQUESTED IN COMPLAINT

☒ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND \$ 5000000

JURY DEMAND: YES ☒ NO ☐

VIII. RELATED CASE(S) IF ANY

(See instruction)

YES ☐ NO ☒

If yes, please complete related case form

DATE: 3/15/2023

SIGNATURE OF ATTORNEY OF RECORD /s/ Gary E. Mason

INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44
 Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil coversheet. These tips coincide with the Roman Numerals on the cover sheet.

- I.** COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.
- III.** CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.
- IV.** CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.
- VI.** CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.
- VIII.** RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should ensure the accuracy of the information provided prior to signing the form.

UNITED STATES DISTRICT COURT

for the

District of Columbia

JENNI SUHR, individually and on behalf of
all others similarly situated,

Plaintiff(s)

v.

DISTRICT OF COLUMBIA HEALTH BENEFIT
EXCHANGE AUTHORITY,
d/b/a DC Health Link,

Defendant(s)

Civil Action No. 1:23-cv-00694

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

District of Columbia Health Benefit Exchange Authority
d/b/a DC Health Link
1225 Eye Street NW, Ste. 400
Washington, D.C. 20005

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Gary E. Mason (DC Bar 418073), Danielle L. Perry (DC Bar 1034960)
MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

ANGELA D. CAESAR, CLERK OF COURT

Date: _____

Signature of Clerk or Deputy Clerk

Civil Action No. _____

PROOF OF SERVICE*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* _____
 was received by me on *(date)* _____.

☐ I personally served the summons on the individual at *(place)* _____
 _____ on *(date)* _____; or

☐ I left the summons at the individual's residence or usual place of abode with *(name)* _____
 _____, a person of suitable age and discretion who resides there,
 on *(date)* _____, and mailed a copy to the individual's last known address; or

☐ I served the summons on *(name of individual)* _____, who is
 designated by law to accept service of process on behalf of *(name of organization)* _____
 _____ on *(date)* _____; or

☐ I returned the summons unexecuted because _____; or

☐ Other *(specify)*:

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

Print

Save As...

Reset