IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
CIVIL DIVISION

RORY LAWLESS, 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. 2023-CAB-001569

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff(s) Rory Lawless ("Plaintiff(s)") bring this action on behalf of themselves and all others similarly situated against Defendant District of Columbia Health Benefit Exchange Authority, dba 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 Rory Lawless is and at all times relevant to this Complaint an individual citizen of the State of Virginia, residing in the city of Arlington. Plaintiff Lawless 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 because this is a class action wherein the amount in controversy exceeds the sum or value of $10,000, exclusive of interest and costs, and the class is so numerous that joinder of all members is impracticable.

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 Court because the District of Columbia is the location 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. DCHL, in the regular course of its business, collects and maintains the Private Information of individuals as a requirement of its business practice.

31. 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.

32. DCHL promises in it its Privacy Policy to "Please be assured that this site is

[11] https://dchealthlink.com/welcome (last accessed Mar. 14, 2023).
[12] https://hbx.dc.gov/node/316092.

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]

33. 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.

34. 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.

35. 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.

36. 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;

[13] Privacy Policy, https://dchealthlink.com/privacy (last visited Mar. 14, 2023).
[14] *Id.*

- 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.

37. 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

38. 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]

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

40. Therefore, ***Plaintiff(s)' and Class Members' PII was in the hands of***

[15] *See* Exhibit A, Plaintiff's Notice Letter.

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.

41. 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]

42. 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.

43. 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]

44. 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.

45. 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]

---

[16] *Id.*
[17] https://dchealthlink.com/privacy (last accessed Mar. 14, 2023).
[18] Notice Letter, Exhibit A.

46. 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.

47. 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.

48. 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

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

50. 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.

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

52. 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
Foreseeable Risk of which Defendant was on Notice

53. 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.

54. 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.

55. 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]

56. 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.

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

58. 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

[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).

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]

59. 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]

60. 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]

61. 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 cybercriminals.

62. 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.

---

[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).

63. 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]

64. 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, DCHLfailed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

65. 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

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

67. 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)

[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.

68. 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.

69. 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 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]

70. The ramifications of Defendant's failure to keep consumers' PII secure are long

[26] 17 C.F.R. § 248.201 (2013).
[27] *Id*.

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

71. 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]

72. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[29]

73. 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 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]

74. Attempting to change or cancel a stolen Social Security number is difficult if not

[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).
[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).

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.

75. 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]

76. 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]

77. 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]

78. 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.

---

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

80. 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.

81. Furthermore, Defendant's credit monitoring offer and advice to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s)(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.

82. 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.

83. 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

84. 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]

85. 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.

86. 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]

87. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[37]

88. 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

[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).
[37] *See* FTC, *Start With Security*, *supra*.

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 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.

89. 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.

90. 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.

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

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. 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.

98. 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.

99. 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.

100. 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.

101. 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

[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).

Members' PII will do so at a later date or re-sell it.

102. 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.

103. 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

104. 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.

105. 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 only limited and short-term effectiveness.

106. 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

[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.

a 2007 report as well ("2007 GAO Report").[41]

107. 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]

108. Theft of Private Information is also gravely serious. PII is a valuable property right.[43]

109. 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.

See 2007 GAO Report, at p. 29.

110. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the

[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).

information on the "cyber black-market" for years.

111. 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 Lawless's Experience

112. Plaintiff Rory Lawless is, and at all times relevant to this complaint, a resident and citizen of the State of Virginia.

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

114. On or about March 9, 2023, Plaintiff Lawless received and email directing him to check for a communication in his DC Health Link account. When he did, the Notice of Data Breach letter was in his file, informing him that his critical PII was "exposed on a public forum."

115. The Notice letter stated that his 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 Lawless Notice of Data Breach Letter, attached as Exhibit A.

116. Plaintiff Lawless is alarmed by the amount of his Personal Information that was stolen or accessed, and even more by the fact that his Social Security number was identified as

among the breach data on DCHL's computer system.

117. 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.

118. For a little over a month now, Plaintiff Lawless has been receiving a combination of around 5–6 spam calls, texts, and many spam emails per day. Prior to this time, he was receiving maybe one troublesome call and/or email per day. He 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.

119. Through DCHL's Notice Letter, Plaintiff Lawless was notified that his Private Information was "publicly exposed" which he assumes means that it has been found on the dark web.

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

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

122. Plaintiff is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

123. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided DCHL with his PII had DCHL disclosed that it lacked data security

practices adequate to safeguard PII.

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

125. 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 his privacy, especially his Social Security number.

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

127. Plaintiff Lawless has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

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

CLASS ACTION ALLEGATIONS

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

130. 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.

131. 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.

132. 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.

133. 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.

134. 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.

135. 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.

136. 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.

137. 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.

138. 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.

139. 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.

140. 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.

141. 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)

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

143. 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.

144. 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.

145. 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.

146. 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.

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

148. 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.

149. 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.

150. 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.

151. 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.

152. 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.

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

154. 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.

155. 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.

156. 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.

157. 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.

158. 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.

159. 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.

160. 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' 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.

161. 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.

162. 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.

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

164. 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).

165. 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.

166. 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.

167. 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.

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

169. 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.

170. 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)

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

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

173. 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.

174. 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.

175. 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.

176. 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.

177. 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.

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

179. 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.

180. 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.

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

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

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

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

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

186. 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)

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

188. 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.

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

190. 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.

191. 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.

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

193. 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.

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

195. 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.

196. 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.

197. 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)

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

199. 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.

200. 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.

201. 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.

202. 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.

203. 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.

204. 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.

205. 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.

206. 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 14, 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)