SCOTT EDELSBERG
CA Bar No. 330990
scott@edelsberglaw.com
EDELSBERG LAW, P.A.
1925 Century Park E #1700
Los Angeles, CA 90067
Telephone: 305.975.3320
Attorney for Plaintiff and Proposed Class

(additional counsel listed on signature page)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

CAREN LUKE, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

CROSSROADS EQUIPMENT LEASE & FINANCE, LLC,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

1. Negligence
2. Negligence *per se*
3. Breach of Implied Contract
4. Invasion of Privacy
5. Breach of Fiduciary Duty
6. Violation of the California Unfair Competition Law
7. Violation of the California Consumer Privacy Act
8. Violation of the California Consumer Records Act
9. Declaratory Judgement

DEMAND FOR JURY TRIAL

Plaintiff Caren Luke, individually, and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant

Crossroads Equipment Lease & Finance, LLC. ("Crossroads" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations on information and belief, except as to her own actions, which are made on personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the recent targeted ransomware attack and data breach ("Data Breach") on Defendant's network that resulted in unauthorized access to the highly sensitive data of roughly 24,000 individuals. As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. Upon information and belief, the specific information compromised in the Data Breach includes, but is not limited to, personally identifiable information ("PII"), such as full names, dates of birth, addresses, Social Security numbers,

driver's license numbers, passport numbers, and tax documents[1].

3. Upon information and belief, up to and through January 2024, Defendant obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network, from which unauthorized actors used an extraction tool to retrieve sensitive PII belonging to Plaintiff and Class Members.

4. Plaintiff's and Class Members' PII—which were entrusted to Defendant, their officials, and agents—were compromised and unlawfully accessed due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network

[1] Sample Notice of Data Security Breach ("Notice") attached hereto as **Exhibit A**.

in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiff's and Class Members' PII.

8. Defendant's failure to safeguard its clients PII is particularly heinous in light of the fact that Defendant suffered the data breach in April 2023 about which it notified its customers nearly a year later in February 2024.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

10. Defendant failed to provide timely, accurate and adequate notice to Plaintiff and Class Members. Plaintiff and Class Members' knowledge about the PII Defendant lost, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by

Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

11. As remediation for allowing Plaintiff's and Class Members' PII to be acquired by an unauthorized third-party, Defendant has stated that "Crossroads is offering two years of 1-bureau free credit monitoring through Experian."[2] To date, Defendant has not contacted or offered any remediation to the victims of this Data Breach, but this assurance serves as tacet acknowledgement of the harm and elevate risk that roughly 24,000 individuals now face as a result of Defendant's acts and omissions.

12. Indeed, armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns 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.

---

[2] *Id.*

13. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present, heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

14. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

16. Accordingly, Plaintiff brings claims on behalf of herself and the Class for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract (iv) invasion of privacy (v) breach of fiduciary duty, (vi) violations of the California Unfair Competition Law, (vii) violations of the California Consumer Privacy Act, (viii) violations of the California Consumer Records Act and (ix) declaratory judgment. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

17. Plaintiff Caren Luke is a natural person, resident, and citizen of California where she intends to remain. She is a Data Breach victim, having applied for transportation equipment leasing through Defendant.

18. Defendant Crossroads Equipment Lease & Finance, LLC is a Limited Liability Company formed in California and with its principal place of business at 9385 Haven Avenue, Rancho Cucamonga, California 91730.

JURISDICTION AND VENUE

19. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 millions, 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[3].

20. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and does substantial business in California.

[3] According to the breach report submitted to the Massachusetts state government, 15 Massachusetts residents were impacted in the Data Breach at Crossroads Equipment Lease & Finance, LLC. See https://www.mass.gov/doc/data-breach-report-2024/download

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND FACTS

A. Defendant's Businesses

22. Defendant is a transportation equipment leasing company and a "national lender with an array of financial products."[4] Defendant advertises $662 million in total assets and $306.1 million in new business volume.[5]

23. On information and belief, Defendant maintain the PII of current and former customers, including but not limited to:

a. name, address, phone number and email address;

b. date of birth;

c. Social Security number;

d. 1099 Forms;

e. Driver's license number, passport number, or other state or

[4] *About Us*, Crossroads, https://www.crlease.com/about-us (last accessed Mar. 26, 2024)

[5] Who We Are, Crossroads, https://www.crlease.com/about-us/who-we-are (last accessed Mar. 26, 2024)

government IDs;

f. Credit or Debit card numbers;

g. Bankruptcy filings;

h. Financial statements and financial account numbers;

i. Credit reports;

j. Loan applications;

k. Medical information; and

l. Digital signatures

m. medication information;

n. health insurance information;

o. photo identification;

p. employment information, and;

q. other information that Defendant may deem necessary to provide its services.

24. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

25. Because of the highly sensitive and personal nature of the information Defendant acquires, stores, and has access to, Defendant, upon information and

belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

27. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

28. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

B. Defendant Fails to Safeguard Consumer PII

29. On or around February 23, 2024, Defendant sending Data Breach Victims a Notice of Data Security Breach letter ("Notice") informing them that:

//

What Happened?

On April 2, 2023, Crossroads became aware that its computer systems were subject to a ransomware attack. As part of the attack, Crossroad's computer systems were encrypted, preventing Crossroads from accessing many of its digital files. This incident impacted Crossroad's ability to complete ACH payments, as well as to perform other important business functions. On January 25, 2024, Crossroads became aware of the nature and scope of the personal information that may have been compromised.

When Did it Happen?

The ransomware attack occurred on April 1, 2023.

What Information Was Involved?

While we have no evidence that your personal information was acquired, the personal information present in the computer systems accessed may have included:

- Name
- Mailing address
- Phone number, mobile and/or home
- Email address
- Date of birth
- Social Security number
- 1099 Forms
- Driver's license number, Passport number, or other state of government IDs (including photocopies of such)
- Vehicle information, such as Vehicle Identification Number or License Plate Number
- Tax documents, including Tax Returns and Tax Forms and individual taxpayer identification number
- Credit or Debit card numbers
- Bankruptcy filings
- Financial statements and financial account numbers plus a security

code, access code, or password that may permit access the account
- Credit reports, including credit score and credit history
- Loan applications
- Medical information
- Digital signatures[6]

30. To date, Defendant's investigation has determined that the private information of roughly 24,000 customers and other affiliated individuals was accessed and compromised by an unauthorized user on or about April 1, 2023.

31. It is likely the Data Breach was targeted at Defendant due to its status as a financial services provider that collects, creates, and maintains sensitive PII.

32. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiff and the Class Members.

33. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff further believes her PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

34. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

[6] Exhibit A.

35. Because of the Data Breach, data thieves were able to gain access to Defendant's private systems on April 1, 2023, and were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.

36. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

37. Plaintiff and the Class Members reasonably relied (directly or indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

38. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

//

//

C. The Data Breach was a Foreseeable Risk and Defendant were on Notice

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

40. In light of recent high profile data breaches at other financial services companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.

41. Defendant knew or should have known that these attacks were common and foreseeable.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

43. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry,

---

[7] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[8] *Id.*

including Defendant.

D. Defendant Fails to Comply with FTC Guidelines

44. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

45. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan

[9] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 23, 2023).

ready in the event of a breach.[10]

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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.

48. These FTC enforcement actions include actions against insurance providers and partners like Defendant.

49. Defendant failed to properly implement basic data security practices.

50. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals'

---

[10] *Id.*

PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

51. Defendant was at all times fully aware of their obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from their failure to do so.

E. Defendant Fails to Comply with Industry Standards

52. As shown above, experts studying cyber security routinely identify insurance providers and partners as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

53. Several best practices have been identified that at a minimum should be implemented by insurance providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

54. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers;

monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

55. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

56. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

F. Defendant's Breach

57. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. failing to adequately protect PII;

c. failing to properly monitor their own data security systems for existing intrusions;

d. failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. failing to protect against reasonably anticipated threats or

hazards to the security or integrity of electronic PII;

j. failing to train all members of their workforces effectively on the policies and procedures regarding PII;

k. failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

m. failing to adhere to industry standards for cybersecurity as discussed above; and,

n. otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

58. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors with unsecured and unencrypted PII.

59. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

//

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

60. Cyberattacks and data breaches at insurance companies and insurance software companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

61. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

62. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or

[11] *See* U.S. GOV. ACCOUNTING OFFICE, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) https://www.gao.gov/new.items/d07737.pdf.

track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

63. The FTC 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.[12]

64. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. Identity thieves can also use Social Security numbers to obtain a

[12] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last accessed Mar. 26, 2024).

driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

66. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[13]

67. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

68. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

[13] *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).

69. According to the U.S. Government Accountability Office, which conducted a study 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.[14]

70. PII is such a valuable commodity to identity-thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

71. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

72. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

73. PII can sell for as much as $363 per record according to the Infosec

[14] GAO Report, at p. 21.

Institute.[15] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

74. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[16] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[17] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

75. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

76. An individual cannot obtain a new Social Security number without

---

[15] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[16] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 26, 2024).

[17] *Id* at 4.

significant paperwork and evidence of actual misuse. Even then, 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."[18]

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."[19]

78. Because of the value of its collected and stored data, the insurance industry has experienced disproportionally higher numbers of data theft events than other industries.

79. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

---

[18] 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.

[19] 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.

H. Plaintiff's and Class Members' Damages

80. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

81. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to two years, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

82. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

83. Plaintiff and Class Members' PII was compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software maintaining PII. This PII was acquired by some unauthorized, unidentified third-party threat actor.

84. Since learning of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

85. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused

by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

86. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

87. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

88. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

89. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

90. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

91. Plaintiff and Class Members may also incur out-of-pocket costs for

protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

92. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

93. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's systems and Plaintiff's and Class Members' PII. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

94. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

95. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts; and

f. closely reviewing and monitoring Social Security numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

96. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

97. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

98. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Luke's Experience

99. Plaintiff Luke provided her information to Defendant as a condition of applying for and/or receiving Defendant's financing services.

100. Plaintiff Luke is very careful about sharing her sensitive Private Information. Plaintiff Luke has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

101. Plaintiff Luke first learned of the Data Breach after seeing a sample on or about February 23, 2024.

102. Based on the information she provided to Defendant, Plaintiff Luke has reason to believe that her PII including, but not limited to, her name, address, phone number, email address, Social Security number, and financial information were compromised in this Data Breach.

103. As a result of the Data Breach, Plaintiff Luke made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

104. Plaintiff Luke has spent significant time and will continue to spend valuable hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

105. Plaintiff Luke suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant maintained belonging to Plaintiff Luke; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

106. As a result of the Data Breach, Plaintiff Luke has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Luke is very concerned about identity theft and fraud, as

well as the consequences of such identity theft and fraud resulting from the Data Breach.

107. As a result of the Data Breach, Plaintiff Luke anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

CLASS ACTION ALLEGATIONS

108. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

109. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

110. Excluded from the Class are Defendant's officers, directors, and employees; 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.

111. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

112. 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 at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

113. 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. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. if 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. if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendant owed a duty to Class Members to safeguard their PII;

f. if Defendant breached their duty to Class Members to safeguard their PII;

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiff and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

114. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

115. Adequacy of Representation. Plaintiff 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.

116. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system 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.

117. 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.

118. 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.

119. Likewise, particular issues under Rule 42(d)(l) 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. if Defendant failed to timely notify the public of the Data Breach;

b. if Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. if Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendant's failure to institute adequate protective security measures amounted to negligence;

e. if Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

120. 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 Defendant.

//

//

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

121. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

122. Plaintiff and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

123. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

124. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII 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.

125. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

126. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

127. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

128. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission 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.

129. 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 are bound by industry standards to protect confidential PII.

130. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. failing to adequately monitor the security of their networks and systems;

d. failing to have in place mitigation policies and procedures;

e. allowing unauthorized access to Class Members' PII;

f. failing to detect in a timely manner that Class Members' PII had been compromised; and

g. failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

131. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant

also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

132. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

133. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

134. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

135. The risk that unauthorized persons would attempt to gain access to

the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

136. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

137. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

138. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

139. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff

and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On behalf of the Plaintiff and the Class)

140. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

141. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

142. Defendant breached its duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

143. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

144. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

145. Plaintiff and Class members were within the class of persons the Federal Trade Commission Act intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

146. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

147. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

148. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

149. Plaintiff hereby repeats and realleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

150. Plaintiff and the Class entrusted their PII to Defendant as a condition of receiving Defendant's services. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

151. At the time Defendant acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

152. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members

from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

153. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

154. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

155. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

156. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised

data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

157. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On behalf of the Plaintiff and the Class)

158. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

159. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

160. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

161. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

162. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

163. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

164. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

165. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

166. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

167. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

168. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

169. Plaintiff, on behalf of themselves and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

170. Plaintiff, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

171. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

172. In providing their PII, directly or indirectly, to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and class members to safeguard and keep confidential that PII.

173. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' and Class Members' personal information as detailed in its Privacy Policy.

174. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers, including Plaintiff and Class members, for the safeguarding of Plaintiffs' and Class members' PII.

175. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its relationship with Defendants' customers, in particular, to keep secure the PII of its customers.

176. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class members' PII.

177. Defendant breached its fiduciary duties to Plaintiffs and class members by otherwise failing to safeguard Plaintiffs' and Class members' PII.

178. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

179. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
[Cal. Bus. & Prof. Code § 17200, et seq. – Unlawful Business Practices]
(On Behalf of Plaintiff and the Class)

180. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this

Complaint and incorporates them by reference herein.

181. Defendant violated Cal. Bus. and Prof. Code § 17200, et seq., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

182. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods for safeguarding the PII of Plaintiff and the Class Members.

183. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

184. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and Class Members were injured and lost money or property,

including but not limited to the price received by Defendant for the products and services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

185. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

186. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

SEVENTH CAUSE OF ACTION
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the Class)

187. Plaintiff repeats and realleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

188. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs and the California Subclass's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

189. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

190. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiffs and California Subclass members' PII. Plaintiff and Class members have an interest in ensuring

that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

191. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

192. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

193. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

//

//

EIGHTH CAUSE OF ACTION
Violations of the California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff and the Class)

194. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this

Complaint and incorporates them by reference herein.

195. Under the California Consumer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believes to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonable believes to have been, acquired by an unauthorized person." *Id.* (emphasis added).

196. The Data Breach constitutes a "breach of the security system" of Defendant.

197. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

198. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class but waited almost eleven months to notify them. Given the severity of the Data Breach, this is an unreasonable delay.

199. Defendant's unreasonable delay prevent Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

200. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

201. Plaintiff and the class are entitled to equitable relief and damages in an amount to be determined at trial.

202. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

NINTH CAUSE OF ACTION
Declaratory Judgement
(On Behalf of Plaintiff and the Class)

203. Plaintiff repeats and re-alleges paragraphs 1 through 120 of this Complaint and incorporates them by reference herein.

204. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

205. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with

respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

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

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

207. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its customers' (i.e., Plaintiff and the Class') data.

208. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

209. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

210. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her 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 the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order;

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such

information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such

third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the

personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are

appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment and post-judgement interest on all amounts awarded;

G. Granting Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial; and

H. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands that this matter be tried before a jury.

Dated: March 26, 2024

Respectfully Submitted,

By: */s/ Scott Edelsberg*

Scott Edelsberg (CA Bar No. 330990)
EDELSBERG LAW, P.A.
1925 Century Park E #1700
Los Angeles, CA 90067
Tel: (305) 975-3320
Email: scott@edelsberglaw.com

Attorney for Plaintiff and Proposed Class