ANDERSON & KARRENBERG
Jared D. Scott (#15066)
50 West Broadway, #600
Salt Lake City, UT 84101-2035
Telephone: (801) 534-1700
jscott@aklawfirm.com

Attorneys for Plaintiff Tyler Whitmore

UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

TYLER WHITMORE, individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **PROGRESSIVE LEASING, LLC,** **Defendant.**	**CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **Case No. _____**

Plaintiff, Tyler Whitmore, individually and on behalf of all similarly situated persons, alleges the following against Progressive Leasing, LLC ("Progressive Leasing" or "Defendant") based on personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated Defendant customers' sensitive information,

including full names, addresses, phone numbers, Social Security numbers, dates of birth, and financial information ("personally identifiable information" or "PII").

2. Defendant leases merchandise for personal, family, and household use, including appliances, furniture, jewelry, electronics, mattresses, mobile devices and accessories, and musical instruments. Defendant provides lease-to-own programs through various retailers throughout the country pursuant to which customers can enter into lease programs to pay for products over time. If a customer completes all lease payment or exercises an early purchase option, they will own the product(s). Customers must provide PII, including their Social Security numbers, bank account details, and credit or debit card information, to apply for the lease program.

3. Upon information and belief, individuals, including Plaintiff and members of the putative class ("Class," defined herein), who wished to receive leasing services from Defendant were required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain services from Defendant, including entering into a lease agreement with Defendant. Defendant retains this information for at least many years and even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On September 11, 2023, Defendant experienced a cybersecurity incident affecting certain of its systems, during which an unauthorized third-party was able to gain access to its network and to certain files containing personal information of some customers and employees

("Data Breach").[1] In response, Defendant launched an investigation, which remains ongoing.[2] The investigation revealed that the unauthorized third-party first gained access to Defendant's network on September 9, 2023.[3] Also, based on the investigation and data analysis, Defendant concluded that the personal information in the stolen documents belonged to Plaintiff, including his name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address.[4] Nearly 200,000 customers were affected by the Data Breach.[5]

6. Defendant failed to adequately protect Plaintiff's and Class members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class members; (ii) warn Plaintiff and Class members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective

[1] *See* Notice of Data Breach Sample Letter, attached hereto as **Exhibit A**.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/84f4c920-079d-4928-896e-977e2bd8ac35.shtml (last visited Oct. 31, 2023).

security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

8. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party.

9. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiff and Class members have suffered injury as a result of Defendant's conduct. These injuries include: (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) and increase in spam calls, texts, and/or emails; 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.

11. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data

security practices.

II. PARTIES

12. Plaintiff is, and at all times mentioned herein was, an individual citizen and resident of Nevada.

13. Defendant is a finance company that generates approximately $2.7 billion in yearly revenue. It is a limited liability company with tis principal place of business located at 256 W. Data Drive, Draper UT 84020.

III. JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of Class members is over 100, many of whom reside outside the state of Utah and have different citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

15. This Court has jurisdiction over Defendant because it operates in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant has harmed Class members residing in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

17. As alleged above, Defendant provides lease-to-own programs through various retailers throughout the country pursuant to which customers can enter into lease programs to pay

for personal, family, and household products over time.

18. Plaintiff and Class members are current and former customers of Defendant.

19. As a condition of receiving its products and/or services, Defendant requires that its customers, including Plaintiff and Class members, entrust it with highly sensitive PII, including Customers must provide PII, including their Social Security numbers, bank account details, and credit or debit card information.[6]

20. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class members.

21. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations (alleged below) to keep such information confidential and secure from unauthorized access.

22. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their PII and demand security to safeguard their PII.

23. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

24. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiff and Class members, to keep their PII confidential and to

[6] *See* https://progleasing.com/how-it-works/ (last visited Oct. 31, 2023).

protect it from unauthorized access and disclosure.

25. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

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 disclosure.

B. *The Data Breach*

27. On or about October 23, 2023, Defendant began sending Notice of Data Breach letters to Class members, stating:

> **What Happened**
>
> On September 11, 2023, we experienced a cybersecurity incident affecting certain Progressive Leasing systems, during which an unauthorized third-party was able to gain access to our network and to certain files containing personal information of some customers and employees. Promptly after detecting the incident, we engaged leading cybersecurity experts and launched an investigation. We also notified law enforcement. Our team is working diligently alongside our cybersecurity experts and with law enforcement to investigate and respond to this incident. While our investigation into the incident, including identification of the data involved, remains ongoing, our preliminary findings indicate that the unauthorized third-party first gained access to our network on September 9, 2023. We are conducting an extensive analysis to determine the individuals whose data was involved in this incident. As part of this review process, on October 9, we identified your personal information among the documents that were acquired without authorization.
>
> **What Information Was Involved**
>
> Based on our investigation and data analysis, the personal information in these stolen documents belonging to you included your name, address, phone number, Social Security number, date of birth, [Extra1], and email address.[7]

[7] *See* Ex. A.

28. Omitted from the Notice are the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class members, who retain a vested interest in ensuring that their PII remains protected.

29. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class members of the Data Breach's critical facts. Without these details, Plaintiff's and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

31. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class members, including their Social Security numbers and other sensitive information. Plaintiff's and Class members' PII was accessed and stolen in the Data Breach.

32. Plaintiff further believes his PII, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.*

33. As a condition to obtain services from Defendant, Plaintiff and Class members were required to give their sensitive and confidential PII to Defendant.

34. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class members' PII, Defendant would be unable to perform its services.

35. By obtaining, collecting, and storing the PII of Plaintiff and Class members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

36. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

37. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class members.

38. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

39. Defendant's negligence in safeguarding the PII of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. *Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of PII Are Particularly Suspectable to Cyber Attacks.*

40. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the breach.

41. Data thieves regularly target companies like Defendant due to the highly sensitive

information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

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.[8]

43. In light of recent 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 the PII that they collected and maintained would be targeted by cybercriminals.

44. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class members as a result of a breach.

45. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class members from being compromised.

46. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members and of the foreseeable

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

consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

47. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially millions of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

48. In the Notice, Defendant offers to provide 12 months of credit monitoring services. This is wholly inadequate to compensate Plaintiff and Class members, as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class members' PII. Moreover, once this service expires, Plaintiff and Class members will be forced to pay out of pocket for necessary identity monitoring services.

49. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems, and that Plaintiff and Class members are currently at risk for identity theft.

50. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

51. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and

Class members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

52. As a corporation in possession of its customers' and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

E. *Value of Personally Identifiable Information*

53. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] 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."[10]

54. The PII of individuals 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.[11]

[9] 17 C.F.R. § 248.201 (2013).
[10] *Id.*
[11] *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 visited Oct. 31, 2023).

55. For example, PII can be sold at a price ranging from $40 to $200.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

56. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names and Social Security numbers.

57. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[14]

58. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

59. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 31, 2023).
[13] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 31, 2023).
[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 31, 2023).

> 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.[15]

F. *Defendant Failed to Comply with FTC Guidelines.*

60. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an 'unfair practice' in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

61. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity 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 their network's vulnerabilities, and implement policies to correct any security problems. 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 into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

62. The FTC further recommends that companies not maintain PII longer than is

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 31, 2023).

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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

65. Defendant was at all times fully aware of its obligation to protect the PII of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Defendant Failed to Comply with Industry Standards.*

66. As noted above, experts studying cybersecurity routinely identify institutions as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

67. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include but are not limited to: educating all employees, strong

password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

68. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

69. 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.

70. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

H. *Defendant Breached Its Duty to Safeguard Plaintiff's and Class members' PII.*

71. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost,

stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class members.

72. 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. 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 that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers PII;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class members' PII.

73. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

74. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class members' confidential PII.

I. *Common Injuries & Damages*

75. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class members has materialized and is present and continuing, and Plaintiff and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

J. *The Data Breach Increases Victims' Risk of Identity Theft.*

76. Plaintiff and Class members are at a heightened risk of identity theft for years to come.

77. Upon information and belief, the unencrypted PII of Class members is for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class members. Unauthorized individuals can easily access the PII of Plaintiff and Class members.

78. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

79. Because a person's identity is akin to a puzzle with multiple data points, 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 track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

80. 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 and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

81. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[16]

[16] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule

82. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

83. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

84. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class members.

85. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

86. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

K. ***Loss Of Time to Mitigate Risk of Identity Theft and Fraud***

87. As a result of the recognized risk of identity theft, when a data breach occurs, and

---

account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Oct. 31, 2023).

an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

88. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and resecuring their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

89. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches 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."[17]

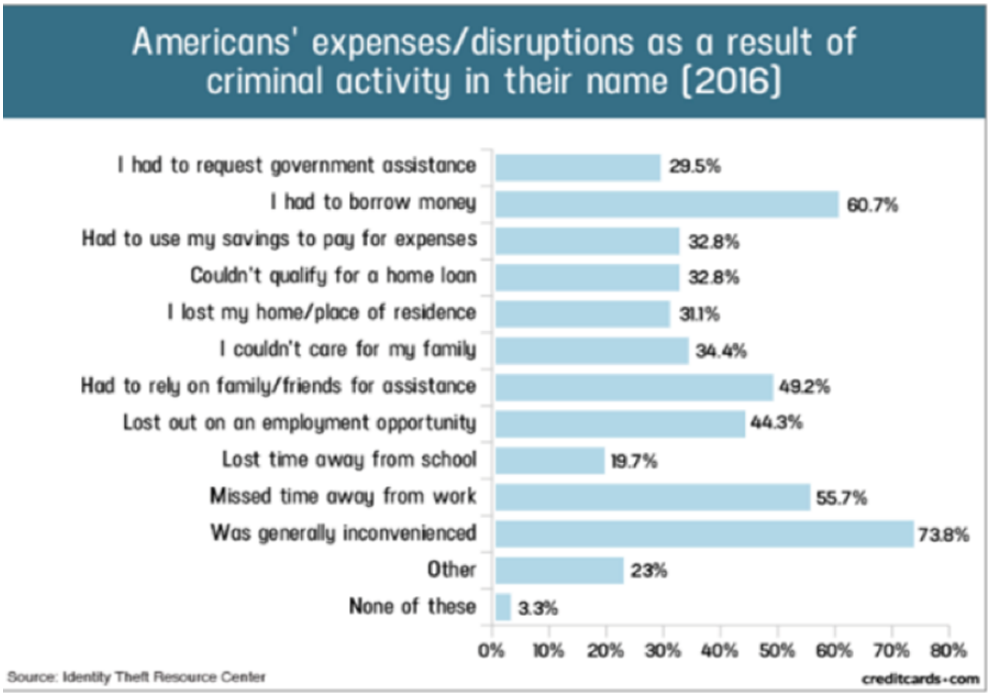
90. These efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years 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.[18]

---

[17] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[18] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Oct. 31, 2023).

91. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[19]



92. And for those Class members who experience actual identity theft and fraud, the GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

L. *Diminution of Value of PII*

93. PII is a valuable property right.[21] Its value is axiomatic, considering the value of

[19] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Oct. 31, 2023).
[20] *See* GAO Report.
[21] *See, e.g.*, Randall 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).

Big Data in corporate America and 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.

94. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[22]

95. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[23,24]

96. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[25]

97. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[26]

98. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing

[22] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Oct. 31, 2023).
[23] https://datacoup.com/ (last visited Oct. 31, 2023).
[24] https://digi.me/what-is-digime/ (last visited Oct. 31, 2023).
[25] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 31, 2023).
[26] *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/ (last visited Oct. 31, 2023).

additional loss of value.

99. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

100. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

101. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

M. *Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.*

102. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, upon information and belief, entire batches of stolen information have been placed on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

103. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her 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.

104. Consequently, Plaintiff and Class members are at a present and continuous risk of fraud and identity theft for many years into the future.

105. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiff and Class members would not need to bear but for Defendant's failure to safeguard their PII.

N. ***Plaintiff's Experience***

106. Plaintiff is a customer of Defendant. While he was temporarily in Tempe, Arizona in May 2023, he shared his PII with Defendant to apply for a loan. Ultimately, Plaintiff was approved for the loan, but he did not accept it.

107. Plaintiff received a Notice of Data Breach letter from Defendant dated October 23, 2023. It states that the breached files included his name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit and email address.

108. Plaintiff has never been part of a data breach and is not aware of any time other than this that his Social Security number, bank information, and income information was exposed, as he diligently protects and maintains his PII.

109. Plaintiff is especially alarmed and anxious that his Social Security number and income information was identified as among the breached data on Defendant's computer system.

110. Plaintiff is reasonably concerned that his PII has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including considering signing up for the credit monitoring services, more often checking his Credit Karma and possibly going back to paying for that service, considering freezing his credit, changing his bank account and passwords, setting up notices and reports, and carefully reviewing all his accounts.

111. In addition, Plaintiff now receives an increased number of spam texts, including text and call from international numbers as well, that he reasonably and temporally attributes to the Data Breach.

112. Plaintiff has spent as many as 40 hours to date obtaining and reviewing the results of his credit monitoring service and additional monitoring of personal and financial accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time he otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Defendant's recommendations.

113. Plaintiff is aware that cybercriminals often sell PII, and once stolen, it is likely to be abused months or even years after the Data Breach.

114. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have trusted Defendant with his PII.

V. CLASS ACTION ALLEGATIONS

115. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

116. Specifically, Plaintiff proposes the following class definition, subject to amendment as appropriate:

> All individuals in the United States whose PII was disclosed in the Data Breach (the "Class").

117. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

118. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

119. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

120. Numerosity. The Class members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

121. 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 engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant's response to the Data Breach was adequate;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class

members' PII;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

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

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

i. Whether Defendant owed a duty to Class members to safeguard their PII;

j. Whether Defendant breached its duty to Class members to safeguard their PII;

k. Whether hackers obtained Class members' PII via the Data Breach;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class members are entitled to damages;

s. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

122. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class members because, *inter alia*, all Class members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class members arise from the same operative facts and are based on the same legal theories.

123. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

124. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class members in that all of Plaintiff's and Class members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

125. Superiority. A Class action is superior to other available methods for the fair and

efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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, conducting 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.

126. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

127. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
Negligence and Negligence Per Se
(On Behalf of Plaintiff and the Class)

128. Plaintiff restates and realleges paragraphs 1 through 127 above as if fully set forth herein.

129. Defendant requires its customers, including Plaintiff and Class members, to

submit non-public PII in the ordinary course of providing its services.

130. Defendant gathered and stored the PII of Plaintiff and Class members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

131. Plaintiff and Class members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

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

133. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

134. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 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.

135. 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 its systems and networks, and the personnel responsible for them, adequately protected the PII.

136. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. That

special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

137. 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 PII.

138. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

139. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

140. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

141. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

142. Defendant breached its duties, pursuant to the FTCA and other applicable standards, 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;

c. Allowing unauthorized access to Class members' PII;

d. Failing to detect in a timely manner that Class members' PII had been compromised;

e. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

143. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

144. Plaintiff and Class members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm it was intended to guard against.

145. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

146. 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 and the Class.

147. A breach of security, unauthorized access, and resulting injury to Plaintiff and

the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

148. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches at large corporations.

149. 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.

150. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

151. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

152. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

153. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

154. Defendant's duty extended to protecting Plaintiff 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.

155. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

156. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

157. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

158. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class 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) and increase in spam calls, texts, and/or emails; 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.

159. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but

not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

160. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, 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 the PII in its continued possession.

161. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

162. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class members in an unsafe and insecure manner.

163. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its 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.

COUNT II
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

164. Plaintiff restates and realleges paragraphs 1 through 127 above as if fully set forth herein.

165. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, (1) to act

primarily for Plaintiff and Class members, (2) for the safeguarding of their PII; (3) to timely notify Plaintiff and Class members of a Data Breach's occurrence and disclosure; and (4) to maintain complete and accurate records of what information (and where) Defendant did and does store.

166. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with its customers, including to keep secure their PII.

167. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiff and Class members on the one hand and Defendant on the other, including with respect to their PII.

168. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

169. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class members' PII.

170. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to timely notify and/or warn Plaintiff and Class members of the Data Breach.

171. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' PII.

172. As a direct and proximate result of Defendant's breaches of its fiduciary duties,

Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost time spent on activities remedying harms resulting from the Data Breach; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) diminution of value of their PII; (v) an increase in spam calls, texts, and/or emails; and (vi) 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) remain 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 their PII.

COUNT III
Breach of Confidence
(On Behalf of Plaintiff and the Class)

173. Plaintiff restates and realleges paragraphs 1 through 127 above as if fully set forth herein.

174. During Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential nature of the PII that Plaintiff and Class members provided to it.

175. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff and Class members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

176. Plaintiff and Class members provided their respective PII to Defendant with the

explicit and implicit understandings that Defendant would protect and not permit the PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

177. Plaintiff and Class members also provided their PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

178. Defendant voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

179. Due to Defendant's failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff's and Class members' confidence and without their express permission.

180. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages, as alleged herein.

181. But for Defendant's failure to maintain and protect Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed

by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Plaintiff's and Class members' PII and the resulting damages.

182. The injury and harm Plaintiff and Class members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiff's and Class members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiff's and Class members' PII had security and other vulnerabilities that placed Plaintiff's and Class members' PII in jeopardy.

143. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) 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, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members, (vii) the diminished value of Representative Plaintiff's and Class Members' PII, and

(viii) the diminished value of Defendant's services for which Representative Plaintiff and Class Members paid and/or received.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

183. Plaintiff restates and realleges paragraphs 1 through 127 above as if fully set forth herein.

184. Plaintiff and Class members conferred a benefit on Defendant. Specifically, they provided Defendant with their PII to apply for leasing services. In exchange, Plaintiff and Class members should have received from Defendant the services that were the subject of the transaction and should have had their PII protected with adequate data security.

185. Defendant knew that Plaintiff and Class members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

186. Defendant failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

187. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

188. If Plaintiff and Class members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained and/or attempted to obtain leasing services from Defendant.

189. Plaintiff and Class members have no adequate remedy at law.

190. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon it.

191. As a direct and proximate result of Defendant's conduct, Plaintiff 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) and increase in spam calls, texts, and/or emails; 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.

192. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

193. Plaintiff and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of himself and Class members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

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' PII, and from refusing to issue prompt, complete and accurate disclosures to 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 their 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 implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class members;

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

vi. 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;

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

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

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

x. 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;

xi. 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;

xii. 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;

xiii. 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;

xiv. 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;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. 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 actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

///

///

///

///

///

Dated: October 31, 2023.

ANDERSON & KARRENBERG

/s/ Jared D. Scott
Jared D. Scott

Kenneth J. Grunfeld
Kristen Lake Cardoso
KOPELOWITZ OSTROW, P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (954) 525-4100
grunfeld@kolawyers.com
cardoso@kolawyers.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org
