M. Anderson Berry, Esq. (SBN 262879)
Gregory Haroutunian, Esq. (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
Email: aberry@justice4you.com;
gharoutunian@justice4you.com

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

DANIEL TOOKER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

U-HAUL INTERNATIONAL, INC.

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

COMPLEX

Plaintiff Daniel Tooker ("Plaintiff" or "Tooker") brings this Class Action Complaint against U-Haul International, Inc. ("U-Haul" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and the investigations of his counsel, and upon information and belief as to all other matters as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") for past and current

customers of Defendant, including, but not limited to their: names, dates of birth, and driver's license numbers or state identification numbers[1].

2. According to Defendant's website, "U-Haul is an American moving truck, trailer, and self-storage rental company, based in Phoenix, Arizona, that has been in operation since 1945."[2]

3. Prior to and through April 5, 2022, Defendant obtained the PII of Plaintiff and Class Members, including the PII of Plaintiff, who was a customer of Defendant, and stored that PII, unencrypted, in an Internet-accessible database on Defendant's network.

4. Defendant's Privacy Policy (the "Privacy Policy") is posted on its website, and it represents, "[w]e use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your information and our systems. We cannot, however, ensure or warrant the security of any information you transmit Us (sic) and you do so at your own risk. However, please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards."[3]

5. On or before August 1, 2022, Defendant learned of a data security incident on its network (the "Data Breach").

6. Defendant determined that, during the Data Breach, an unknown actor compromised two unique passwords for accessing Defendant's copies of contracts with Defendant's past customers, which includes Plaintiff and Class Members.

7. On or around September 9, 2022, Defendant notified the United States Securities and Exchange Commission ("SEC") of the Data Breach.

8. On or around September 9, 2022, Defendant began notifying Class Members of the Data Breach, including Plaintiff.[4]

---

[1] Personally identifiable information is generally compromised of information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifiable information. 2 C.F.R. § 200.79.
[2] *See* https://www.uhaul.com/About/History/ (last visited Sept. 19, 2022).
[3] *See* https://www.uhaul.com/Legal/PrivacyPolicy/ (last visited Sept. 21, 2022).
[4] *U-Haul Notice of Data Breach*, State of California Department of Justice, Rob Bonita,

9. 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 their information against unauthorized access and intrusion. Moreover, Defendant admits that the unencrypted PII accessed by an unauthorized actor included name, date of birth, and driver's license number or state identification number.

10. Plaintiff's and Class Members' PII can be sold on the dark web. Hackers can access and sell the unencrypted, unredacted PII to criminals, leaving Plaintiff and Class Members virtually defenseless to these cyber criminals. Now Plaintiff and Class Members face a lifetime risk of (i) identity theft, which is heightened by the loss of driver's license numbers or state identification numbers, and (ii) the sharing or detrimental use of their sensitive information.

11. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited almost months after the Data Breach allegedly ended to report it to the SEC and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

12. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

13. 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

---

Attorney General, https://oag.ca.gov/system/files/U-Haul%20-%20California%20Notification.pdf, (last visited on Sept. 19, 2022).

reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, 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) may 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 the PII.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement 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 the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. 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.

II. PARTIES

16. Plaintiff Daniel Tooker is a citizen and resident of Oklahoma residing in Norman, Oklahoma.

17. Defendant is a Nevada Corporation with a principal place of business in Phoenix, Arizona and is a subsidiary of AMERCO, Inc., also a Nevada Corporation.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged

herein are currently unknown to Plaintiff. Therefore, Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

III. JURISDICTION AND VENUE

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

21. Defendant is a citizen of Nevada and Arizona because it is a corporation formed under Nevada law, and its principal place of business is in Phoenix, Arizona.

22. The District of Arizona has personal jurisdiction over Defendant because Defendant conducts substantial business in Arizona and this District.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District, and a substantial part of the errors, events, or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. THE DATA BREACH WAS FORESEEABLE

24. Plaintiff and Class Members, who are past and current customers of Defendant, provided and entrusted Defendant with sensitive and confidential information, including their names, dates of birth, and driver's license or state identification numbers.

25. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes

only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

26. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

i. The Data Breach

27. On or about September 9, 2022, Defendant sent Plaintiff and Class Members a *Notice of Recent Security Incident*.[5] Defendant informed Plaintiff and other Class Members that:

> **What Happened?**
>
> We detected a compromise of two unique passwords that were used to access a customer contract search tool that allows access to rental contracts for U-Haul customers. The search tool cannot access payment card information; no credit card information was accessed or acquired. Upon identifying the compromised passwords, we promptly changed the passwords to prevent any further unauthorized access to the search tool and started an investigation. Cybersecurity experts were engaged to identify the contracts and data that were involved. The investigation determined an unauthorized person accessed the customer contract search tool and some customer contracts. None of our financial, payment processing or U-Haul email systems were involved; the access was limited to the customer contract search tool.
>
> **What Information Was Involved?**
>
> On August 1, 2022, our investigation determined some rental contracts were accessed between November 5, 2021, and April 5, 2022. After an in-depth analysis, our investigation determined on September 7, 2022, the accessed information includes your name and driver's license or state identification number.
>
> **What We Are Doing?**
>
> The safety and trust of our customers, including the protection of personal information, is a top priority for U-Haul Company and we take that responsibility very seriously. While the information accessed in this incident did not include payment card information, we fully understand this is an inconvenience to you. We sincerely apologize for that. Please know we are

[5] *Id.*

> working diligently to further augment our security measures to guard against such incidents and implementing additional security safeguards and controls on the search tool.

28. Defendant also filed a notice with the SEC in its parent company (AMERCO)'s Annual Report advising that the PII impacted included names, dates of birth, driver's license numbers, or state identification numbers.[6]

29. Defendant also admitted, in the *Notice of Recent Security Incident*, that an unauthorized actor accessed sensitive information about Plaintiff and Class Members, including names, date of births, driver's license numbers or state identification numbers.

30. In response to the Data Breach, Defendant claims that cybersecurity experts are "implementing additional security safeguards and controls to prevent further such incidents."[7] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected. In short, mystery shrouds this Data Breach, which further exposes Plaintiff and Class Members to continued harm.

31. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply 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 and use it to exploit and steal from Plaintiff and Class Members for the rest of their lives because of Defendant's carelessness.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

---

[6] AMERCO 2021 Annual Report, available at https://www.amerco.com/reports.aspx (last visited Sept. 20, 2022).

[7] *U-Haul Notice of Data Breach*, State of California Department of Justice, Rob Bonita, Attorney General, https://oag.ca.gov/system/files/U-Haul%20-%20California%20Notification.pdf, (last visited on Sept. 20, 2022).

33. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information. Instead, it left the vast troves of PII it collected from Plaintiff and Class Members lying in wait for cybercriminals.

34. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet. Cautionary corporate tales of huge data breaches abounded, tales that should have been heeded by any responsible business entity, which valued its customers.

35. Prior to the Data Breach, as part of its parent company's annual report filed with the SEC in July 2021, Defendant acknowledged, in a statement that now rings hollow and prophetic at the same time, that:

> Our information systems are largely Internet-based, including our point-of-sale reservation system, payment processing and telephone systems. While our reliance on this technology lowers our cost of providing service and expands our abilities to better serve customers, it exposes us to various risks including natural and manmade disasters, terrorist attacks and cyber-attacks. **We have put into place extensive security protocols, backup systems and alternative procedures to mitigate these risks.** However, disruptions or breaches, detected or undetected by us, for any period of time in any portion of these systems could adversely affect our results of operations and financial condition and inflict reputational damage.
>
> In addition, the provision of service to our customers and **the operation of our networks and systems involve the storage and transmission of proprietary information and sensitive or confidential data, including personal information of customers,** system members and others. Our information technology systems may be susceptible to computer viruses, attacks by computer hackers, malicious insiders, or catastrophic events. Hackers, acting individually or in coordinated groups, may also launch distributed denial of service attacks or ransom or other coordinated attacks that may cause service outages or other interruptions in our business and access to our data. **In addition, breaches in security could expose us, our customers, or the**

> **individuals affected, to a risk of loss or misuse of proprietary information and sensitive or confidential data.** The techniques used to obtain unauthorized access, disable or degrade service or sabotage systems change frequently, may be difficult to detect for a long time and often are not recognized until launched against a target. As a result, we may be unable to anticipate these techniques or to implement adequate preventative measures.
>
> Any of these occurrences could result in disruptions in our operations, the loss of existing or potential customers, damage to our brand and reputation, and litigation and potential liability for the Company. In addition, the cost and operational consequences of implementing further data or system protection measures could be significant and our efforts to deter, identify, mitigate and/or eliminate any security breaches may not be successful. (emphasis added) [8]

36. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

37. Prior to the Data Breach, Defendant knew or should have known that it erred when it failed to encrypt the names, driver's license numbers or state identification numbers, and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

ii. Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

38. As a condition of being a past or current customer of Defendant, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential PII.

38. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

39. 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 it was responsible for protecting the PII from disclosure.

[8] AMERCO 2021 Annual Report, available at https://www.amerco.com/reports.aspx (last visited Sept. 20, 2022).

40. 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 securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

iii. Securing PII and Preventing Breaches

41. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the PII it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

42. 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, ones which it clearly was aware of before the date breach. *See* §(IV)(A)(i) *supra*. Despite the prevalence of public announcements of data breach and data security compromises, and its awareness of the risks, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

43. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[9]

44. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years, including high-profile breaches for Equifax, Target, and various healthcare systems.[10] This is especially true because Defendant collects much of the same PII that financial institutions, healthcare providers, and insurers collect, which includes, but is not limited to, names, addresses, credit card information, drivers' license numbers or state identification numbers, and dates of birth. Because they collect this PII and

[9] *2019 End of Year Data Breach Report,* Identity Theft Center (2019), https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Sept. 20, 2022).

[10] Michel Hill and Dan Swinhoe, *The 15 biggest data breaches of the 21st century*, CSO, (Sept.12, 2021), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Sept. 19, 2022).

let it be known that they collect this PII they are targeted by the same kinds of cybercriminals who target financial institutions, healthcare systems, and insurance companies. This targeting combined with Defendant's lax security measures made them a prime target for cybercriminals, and it was one of the reasons this data breach was not only foreseeable but, unfortunately, inevitable.

45. Drivers' license numbers are perhaps some of the most coveted of all PII sought by cybercriminals. In 2021 alone, drivers' license numbers were taken from auto-insurance providers by cybercriminals in attacks on many companies that collect similar PII to Defendant, including GEICO, Farmers, USAA, Kemper, Metromile, and American Family. This targeting of the auto-insurance industry and companies who gather and store driver data such as drivers' license numbers demonstrates that the PII companies like Defendant gather and possess is in high demand by cybercriminals. Likewise, sophisticated multi-national companies like Defendant knew or should have known that their security practices were of particular importance to safeguard consumer data.[11]

46. In the first half of 2021, there were 846 data breaches in the country, on pace to set a new record. These data breach incidents impacted nearly 52.8 million individuals.[12]

47. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

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

I. [11] ***Data Breaches Are Up 38 Percent in Q2 2021; The Identity Theft Resource Center Predicts a New All-Time High by Year's End*, Identity Theft Resource Center (July 8, 2021),** https://www.idtheftcenter.org/post/data-breaches-are-up-38-percent-in-q2-2021-the-identity-theft-resource-center-predicts-a-new-all-time-high-by-years-end/ (last visited Sept. 19, 2022).

49. The New York Department of Financial Services ("NYSDFS"), in their February 16, 2021 industry letter recommended the following steps for entities that maintain public-facing websites:

a. Conduct a thorough review of public-facing website security controls, including but not limited to a review of its Secure Sockets Layer (SSL), Transport Layer Security (TLS), and HTTP Strict Transport Security (HSTS and Hypertext Markup Language (HTML) configurations.

b. Review public-facing websites for browser web developer tool functionality. Verify and, if possible, limit the access that users may have to adjust, deface, or manipulate website content using web developer tools on the public-facing websites.

c. Review and confirm that its redaction and data obfuscation solution for NPI is implemented properly throughout the entire transmission of the NPI until it reaches the public-facing website.

d. Ensure that privacy protections are up to date and effectively protect NPI by reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides.

e. Search and scrub public code repositories for proprietary code.

f. Block the IP addresses of the suspected unauthorized users and consider a quote limit per user session.[13]

50. Due to the "ongoing cybercrime campaign that is a serious threat to consumers," NYSDFS issued a Cyber Fraud Alert Follow-up on March 30, 2021. They urged "**personal lines insurers and other financial services companies to avoid displaying prefilled NPI on public-facing websites considering the serious risk of theft**

[13] Industry Letter, *supra*, note 1. Note that this Industry Letter was reported online on numerous websites, including: https://digitalguardian.com/blog/public-facing-financial-services-sites-ripe-data-theft(Feb. 23, 2021); https://www.gravoc.com/2021/04/09/cyber-fraud-alert-issued-for-websites-collecting-npi/ (Apr. 9, 2021); and https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (Feb. 16, 2021) (last visited on Sept. 19, 2022).

and consumer harm. (Emphasis in original) We note that many of the auto insurers targeted by this cybercrime campaign have recently disabled all NPI prefill on their public-facing websites."[14]

51. NYSDFS also recommended the following basic security steps be implemented:

g. **Disable prefill of redacted NPI.** Avoid displaying prefilled NPI, especially on public facing websites.

h. **Install Web Application Firewall (WAF).** WAFs help protect websites from malicious attacks and exploitation of vulnerabilities by inspecting incoming traffic for suspicious activity.

i. **Implement CAPTCHA.** Cybercriminals use automated programs or "bots" to steal data. Completely Automated Public Turing Tests ("CAPTCHA") attempt to detect and block bots.

j. **Improve Access Controls for Agent Portals**. Agent portals typically allow agents access to consumer NPI, and robust access controls are required by DFS's cybersecurity regulation.

k. **Training and awareness**. Employees and agents should be trained to identify social engineering attacks. Employees and agents should know not to disclose NPI, including DLNs, over the phone. Robotic scripts with grammatical errors or repeated statements used during dialogue are key identifiers of fraudulent calls.

l. **Limit access to NPI**. Employees and agents should only have access to sensitive information that is necessary to do their job.

m. **Wait until payments have cleared before issuing a policy**. Auto insurers should consider waiting until an eCheck, credit card, or debit card payment

[14]Industry Letter, New York Department of Financial Services Industry Letter (Mar. 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup, (last visited Sept. 19 2022).

has been cleared by the issuing bank before generating an online policy and granting the policyholder access to NPI.

n. **Protect NPI received from data vendors.** Ensure that APIs used to pull data files, including JSON and XML, from data vendors are not directly accessible for the internet or agent portals.[15]

52. For these reasons, as this information is relevant to any entity that handles PII, Defendant knew or should have known about these dangers and strengthened its data protection and computer system/network accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

53. Defendant knowingly refrained from implementing basic security measures to protect Plaintiff's and Class Members' PI, including motor vehicle records, in spite of having control over the configuration and design of their online quoting platform.

B. DEFENDANT FAILED TO FOLLOW FTC GUIDELINES

54. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses to 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.

55. 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 patient 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.[16] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all

[15] *Id.*

[16] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 20, 2022).

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 ready in the event of a breach.[17]

56. 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.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

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

59. Defendant failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

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

C. DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS

61. Several best practices have been identified that at a minimum should be implemented by companies 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.

[17] *Id.*

62. Other best cybersecurity practices that are standard in the Defendant's industry, and that upon information and belief Defendant did not employ, 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; and training staff regarding critical points.

63. 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.

64. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

D. DEFENDANT'S BREACH

65. 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 data. 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;

b. Failing to adequately protect consumers' PII;

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

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

66. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access their IT systems which contained unsecured and unencrypted PII.

67. Accordingly, as outlined below, Plaintiff and Class Members now face a present and increased risk of fraud and identity theft.

E. HARM TO CONSUMERS

68. 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.

69. Specifically, driver's license numbers are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[18]

70. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's

[18]Lee Matthews, *Hackers Stole Customers' License Numbers in Months-Long Breach,* Forbes (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658. (last visited on Sept. 19, 2022).

> license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[19]

71. According to cyber security specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[20] However, this is not the case. As cyber security experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[21]

72. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[22]

73. 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 a present and increased risk of fraud and identity theft for many years into the future. Accordingly, Plaintiff and Class Members must vigilantly guard against identity theft for many years to come.

74. Identity theft resulting from the Data Breach may not come to light for years.

---

[19] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (Oct. 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Sept. 19, 2022).

[20] Scott Ikedia, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims,* CPO Magazine (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Sept. 19, 2022).

[21] *Id.*

[22] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed Sept. 19, 2022).

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

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

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

F. HARM TO PLAINTIFF

Plaintiff Daniel Tooker's Experience

78. Plaintiff was required to provide and did provide his PII to Defendant. The PII included his name, date of birth, address, email address, telephone number, and driver's license number.

79. To date, U-Haul has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach, offering only an optional subscription to Equifax's Identity Theft Protection program.

80. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members' PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class

Members by requiring them to expend time signing up for the service and addressing timely issues when the service number for enrollment does not work properly.

81. Plaintiff and Class Members have been further damaged by the compromise of their PII.

82. Plaintiff Tooker's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed U-Haul International's network for the specific purpose of targeting the PII.

83. Plaintiff Tooker typically takes measures to protect his PII and is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

84. Plaintiff Tooker stores any documents containing his PII in a safe and secure location. And he diligently chooses unique usernames and passwords for his online accounts.

85. As a result of the Data Breach, Plaintiff has diligently monitored his credit and financial accounts, while constantly worrying about what his PII could be used for in the future by any third-party with access to the dark web.

86. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

87. Since the Data Breach, Plaintiff has also experienced a substantial increase in phishing attacks on his email account, as well as a sharp increase in spam to his phone in the form of texts and calls.

88. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

89. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

90. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his driver's license number, being placed in the hands of criminals.

91. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he received services from Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

92. As a result of 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. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

93. Plaintiff brings this action individually and on behalf of all other persons similarly situated. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose Personally Identifiable Information was maintained on Defendant's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class").

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

95. **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 over 2.1 million individuals whose sensitive data was compromised in the Data Breach.

96. **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 the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and

Class Members' PII;

b. Whether the Defendant violated federal or state law with respect to the allegations made herein;

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

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

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

f. Whether Defendant's owed a duty to Class Members to safeguard their PII;

g. Whether Defendant's breached a duty to Class Members to safeguard their PII;

h. Whether computer hackers obtained Class Members PII in the Data Breach;

i. Whether the Defendant knew or should have known that their data security systems and monitoring processes were deficient;

j. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant violated the DPPA; and

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

97. **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.

98. **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.

99. **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 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.

100. **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.

101. 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.

V. COUNTS

COUNT I
VIOLATION OF THE DRIVER'S PRIVACY PROTECTION ACT
18 U.S.C. § 2721, *et seq.*
(On Behalf of Plaintiff and the Class)

102. Plaintiff and the Class reallege and incorporate by reference paragraphs 1-101 as if fully alleged herein.

103. The Driver's Privacy Protection Act (the "DPPA") provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

104. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

105. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(1).

106. The DPPA defines "personal information" as "information that identifies an individual, including an individual's photograph, social security number, driver

identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information..." 18 U.S.C. § 2725(3).

107. Drivers' licenses are motor vehicle records which, and the drivers' license numbers ("driver identification number") contained on them qualify as personal information under the DPPA.

108. Defendant obtains, uses, discloses, resells, and rediscloses personal information from its customers' motor vehicle records, including, but not limited to, drivers' license numbers, that they obtain directly from motor vehicle records agencies.

109. Defendant also obtains customers' motor vehicle records through resellers who sell such records.

110. Defendant knowingly used motor vehicle records for uses not permitted by the DPPA, including sales, and marketing, among other impermissible uses.

111. Defendant knowingly failed to protect its computer systems and/or linked its respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiff's and Class Members' personal information, including the application website.

112. During the time period starting on or before November 5, 2021, Defendant made Plaintiff and Class Members' personal information, including drivers' license numbers, available to thieves who removed that personal information from Defendant's computer systems. Defendant knowingly used and disclosed and/or redisclosed Plaintiff's and Class Members' motor vehicle records and the personal information contained therein to thieves, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

113. As a result of the Unauthorized Data Disclosure, Plaintiff and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

///

COUNT II
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

114. Plaintiff and the Class reallege and incorporate by reference paragraphs 1-101 as if fully alleged herein.

115. Defendant owed Plaintiff and the Class Members the duty of reasonable care, which included, but was not limited to, protecting their PII.

116. Defendant obtained Plaintiff's and Class Members' PII, including but not limited to their name and drivers' license numbers or state identification numbers.

117. As a condition of being past and current customers of Defendant, Plaintiff and Class Members were obligated to provide and entrust Defendant with certain PII.

118. Plaintiff and Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to third parties.

119. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant had and/or voluntarily undertook a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft.

120. More specifically, Defendant's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

121. Defendant also owed a duty of care to Plaintiff and the Class Members to provide security consistent with industry standards, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' information.

122. Defendant knew or reasonably should have known that the failure to exercise reasonable care in collecting, storing, and using of the PII of Plaintiff and Class Members involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

123. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the Class Members from a data breach. Defendant breached its duty by failing to use reasonable measures to protect Plaintiff's and Class Members' PII.

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

125. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class Members during the time the PII was within Defendant's possession or control.

126. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

127. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class Members in the face of increased risk of theft.

128. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

129. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

130. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class Members the existence and scope of the Data Breach.

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

132. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and the Class Members. The PII of Plaintiff and the Class Members 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.

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

134. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class Members 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.

135. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class Members 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 fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

136. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

137. Plaintiff realleges and incorporates by reference paragraphs 1-101 as if fully alleged herein.

138. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

139. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

140. Defendant's duty to use reasonable security measures also arose under the DPPA, under which Defendant was required to protect the privacy, confidentiality, and integrity of drivers' license information and only to use drivers' license information in a permissible fashion.

141. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) along with the DPPA constitutes negligence *per se*.

142. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the DPPA, were intended to protect.

143. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the DPPA were intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and Class Members. The DPPA was similarly enacted as a direct result of failures to protect consumer privacy like those outlined above.

144. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and the Class;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. 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 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 its security personnel regarding any new or modified procedures;

ix. 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;

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

xi. 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;

xii. 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;

xiii. requiring Defendant to implement a system of tests to assess its 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;

xiv. 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;

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

xvi. 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;

E. Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages and compensatory damages, as allowable by law;

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

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

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

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

JURY TRIAL DEMAND

Jury trial is demanded by Plaintiff and members of the putative Class.

DATED: September 23, 2022

Respectfully submitted,

By: _____

M. ANDERSON BERRY
(*pro hac vice* forthcoming)
GREGORY HAROUTUNIAN
(*pro hac vice* forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
Email: aberry@justice4you.com
gharoutunian@justice4you.com