Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: (602) 730-7100
Facsimile: (623) 235-6173

Attorneys for Plaintiffs and the Proposed Class
[Additional counsel on signature page]

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Michelle Anderson; Saray Hendricks; Peter Telford; Hulises Rolon; Denise Bowen; Bryan Bowen; Mark Johnson; Gerardo Rivera; and Ariana Allen, individually and on behalf of themselves and all others similarly situated, Plaintiffs, v. U-Haul International Incorporated, Defendant.	Lead Case No.: 2:22-cv-01565-MTL Consolidated with: Case No.: 2:22-cv-01608; Case No.: 2:22-cv-01625; Case No.: 2:22-cv-01631; Case No.: 2:22-cv-01658; Case No.: 2:22-cv-01693. **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Michelle Anderson, Saray Hendricks, Peter Telford, Hulises Rolon, Denise Bowen, Bryan Bowen, Mark Johnson, Gerardo Rivera ("2022 Plaintiffs"), and Ariana Allen ("Plaintiff Allen") (collectively, "2022 Plaintiffs" and "Plaintiff Allen" shall be referred to as "Plaintiffs" unless otherwise specified) bring this Second Amended Consolidated Class Action Complaint against U-Haul International, Inc. ("U-Haul" or "Defendant"), individually and on

behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII" or "Private Information")[1] 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.

2. According to Defendant's website, Defendant "is an American moving truck, trailer, and self-storage rental company, based in Phoenix, Arizona, that has been in operation since 1945."[2] Defendant is one of the largest and most recognizable companies in the consumer moving and storage industry with revenues of $4.54 billion for the fiscal year ending in 2021.[3]

3. As a regular and necessary part of its business, Defendant acquires and stores vast amounts of sensitive and non-public consumer data.

4. Prior to and through December 5, 2023, Defendant obtained the PII of Plaintiffs and Class Members, who were customers of Defendant, and stored that PII unencrypted and in an Internet-accessible environment on Defendant's network.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *See* https://www.uhaul.com/About/History/ (last visited Apr. 23, 2024).

[3] *See* https://finance.yahoo.com/news/uhal-amerco-crosses-4-billion-092300411.html (last visited Apr. 23, 2024).

5. Defendant understands the need to safeguard the PII that it collects and maintains for its pecuniary benefit, and Defendant's Privacy Policy (the "Privacy Policy"), posted on its website, represents that it "[u]ses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your Information and our systems."[4]

6. Despite this, Defendant suffered not one, but two separate but almost identical data incidents that it learned about on July 12, 2022 and December 5, 2023, respectively.

7. Specifically, on July 12, 2022, Defendant learned of a data incident on its network and determined that an unknown actor compromised two unique passwords for accessing Defendant's contract search tool and accessed the contracts of Defendant's past and current customers, including the 2022 Plaintiffs and Class Members (the "2022 Data Incident"). Yet again, on December 5, 2023, Defendant learned of another almost identical data incident on its network and determined that an unknown actor used stolen credentials to access a system Defendant and its employees used to track customer reservations and was able to access and exfiltrate customer records containing the sensitive PII of Defendant's past and current customers, including Plaintiff Allen and Class Members (the "2023 Data Incident") (collectively, the "2022 Data Incident" and the "2023 Data Incident" shall be referred to as the "Data Incidents" unless otherwise specified).

8. On or around September 9, 2022, Defendant notified the U.S. Securities and Exchange Commission ("SEC") of the 2022 Data Incident.

9. On or around September 9, 2022, nearly two months after discovering the 2022

[4] *See* https://www.uhaul.com/Legal/PrivacyPolicy/#Security (last visited Apr.213, 2024).

Data Incident, Defendant began notifying the 2022 Plaintiffs and Class Members that their PII had been compromised in the 2022 Data Incident.

10. On or around February 22, 2024, more than three months after discovering the 2023 Data Incident, Defendant reported the 2023 Data Incident to the Office of the Maine Attorney General and began notifying Plaintiff Allen and Class Members that their PII had been compromised in the 2023 Data Incident.[5]

11. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Without the PII of Plaintiffs and Class Members, Defendant would have been unable to provide rental or storage services to consumers. Defendant admits that the unencrypted PII accessed by an unauthorized actor included names, dates of birth, and drivers' license numbers or state identification numbers.

12. The exposed PII of Plaintiffs and Class Members has been published and will likely be sold on the dark web to identity thieves. Hackers target companies like Defendant to access and then offer for sale the unencrypted, unredacted PII they maintain to other criminals. This is evidenced by the fact that shortly after the 2022 Data Incident, William Frierson received a notification that his PII was located on the dark web. Plaintiffs and Class Members now face an ongoing and lifetime risk of identity theft, which is heightened here by the loss of driver's

---

[5] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/8cbdef9d-3c2c-48e1-b36e-d202df6bd1af.shtml (last visited Apr. 23, 2024).

license numbers or state identification numbers in conjunction with verifying information like the names and dates of birth of Plaintiffs and Class Members.

13. The PII was targeted and compromised by criminals due to Defendant's negligent and/or careless acts and omissions regarding the condition of its data security practices and the failure to protect the PII of Plaintiffs and Class Members. In addition, Defendant waited nearly two months after the 2022 Data Incident occurred to report it to the SEC and affected individuals, and more than three months after the 2023 Data Incident occurred to report it to the Office of the Maine Attorney General and affected individuals, which prevented them from taking efforts to timely mitigate the consequences of the Data Incidents.

14. As a result of this delayed response, Plaintiffs 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. This risk will remain for their respective lifetimes because the information compromised in the Data Incidents is immutable and impossible to change, (i.e., names and dates of birth) and is often used to verify an individual's identity.

15. Plaintiffs bring this action on behalf of all persons residing in California whose PII was compromised as a result of Defendant's failure to adequately protect the PII of Plaintiffs and Class Members and to timely notify them of the Data Incidents after they occurred. Defendant's conduct amounts at least to a violation of the California Consumer Privacy Act (CCPA).

16. Plaintiffs 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 Incidents, including but not limited to lost time; (iv) the disclosure of their Private Information; and (v) the present, 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.

17. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs 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 concerning data security and failing to enact policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to unauthorized third parties. Plaintiffs 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

18. Plaintiff Michelle Anderson is a citizen of California residing in Sacramento, California.

19. Plaintiff Saray Hendricks is a citizen of California residing in Murrietta, California.

20. Plaintiff Peter Telford is a citizen of California residing in San Diego, California.

21. Plaintiff Hulises Rolon is a citizen of California residing in Fresno, California.

22. Plaintiff Denise Bowen is a citizen of California residing in Lancaster, California.

23. Plaintiff Bryan Bowen is a citizen of California residing in Sonora, California.

24. Plaintiff Mark Johnson is a citizen of California residing in Manteca, California.

25. Plaintiff Gerardo Rivera is a citizen of California residing in Sonora, California.

26. Plaintiff Ariana Allen is a citizen of California residing in Sacramento, California.

27. Defendant is a Nevada corporation with a principal place of business located at 2727 North Central Avenue in Phoenix, Arizona.

28. 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 Plaintiffs. Plaintiffs 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.

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

III. JURISDICTION AND VENUE

30. 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 of 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 is a citizen of a state different from Defendant to establish minimal diversity.

31. 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.

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

33. 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 events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members

34. Plaintiffs 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 numbers or state identification numbers. Defendant required that it be entrusted with this PII as a condition of providing its services.

35. Defendant used Plaintiffs' and Class Members' PII to derive a substantial portion of its revenue. Without the PII of Plaintiffs and Class Members, Defendant would have been unable to provide services to Plaintiffs and Class Members.

36. Plaintiffs and Class Members value the integrity of their PII and expect reasonable security to safeguard their PII. Plaintiffs and Class Members relied on the sophistication of Defendant, an industry leading company, 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.

37. As a result of collecting and storing the PII of Plaintiffs and Class Members for its own pecuniary benefit, Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The 2022 Data Incident

38. On or about September 9, 2022, Defendant sent the 2022 Plaintiffs and Class Members a letter titled *Notice of Recent Security Incident* (the "Notice"). Defendant's Notice letter informed the 2022 Plaintiffs and Class Members:

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

39. Defendant also filed a notice with the SEC advising that the compromised PII included names, dates of birth, and driver's license numbers.[6]

40. Defendant admitted in both the Notice letter and the SEC filing that an unauthorized actor accessed sensitive information about the 2022 Plaintiffs and Class Members, including their names, dates of birth, and driver's license numbers or state identification numbers.

41. Defendant has publicly stated that it first identified that two of its passwords were compromised on July 12, 2022.[7] Once the passwords were compromised, the attackers were able to access an unencrypted, internet accessible database of rental contracts containing the PII of Defendant's customers.

42. In an online FAQ titled "What has U-Haul done thus far to resolve the issue," Defendant simply states that "Upon discovery, we changed the passwords and implemented

---

[6] *See* Form 8-K, filed by AMERCO on September 9, 2022, available at https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/4457/000000445722000081/uhal-20220909.htm (last visited March 13, 2024). AMERCO was the parent company of Defendant until on or around December 19, 2022, when AMERCO changed its name to U-Haul Holding Company.

[7] *See* https://www.uhaul.com/Update/ (last visited Apr. 23, 2024).

additional safeguards and controls for accessing the search tool."[8] It further states that based on this simple "remediation of the incident, we are confident there is no further risk to our systems and the data contained within."[9] Notably, Defendant makes no mention of how the passwords were compromised and whether that avenue of attack has been properly identified and addressed.

43. Defendant has also stated that cybersecurity experts "are implementing additional security safeguards and controls to prevent further such incidents."[10] However, the details of those safeguards and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or the 2022 Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

44. Other than the statement that the 2022 Data Incident involved the "compromise of two unique passwords," and that Defendant secured its systems by changing these passwords more than seven months after the 2022 Data Incident was initiated, U-Haul has not shared many details regarding the cause of the 2022 Data Incident. However, the fact that threat actors gained access through two unique passwords indicates that the 2022 Data Incident was effectuated through phishing or other rudimentary social engineering techniques.[11] Phishing is among the most used methods cybercriminals use to obtain passwords and infiltrate corporate data records.

---

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *See* https://www.jdsupra.com/legalnews/u-haul-international-inc-files-notice-3404267/ (last visited March 13, 2024); *see also* https://www.sparefoot.com/self-storage/news/11891-u-haul-notifies-customers-of-major-data-breach/ (last visited Apr. 23, 2024).

In such an attack, the hacker tricks a legitimate user into inputting their password into a fake website designed to look official. A link to the fake site is often sent by e-mail, with the sender impersonating someone the victim knows and trusts. Defendant could have prevented such an attack by adequately training employees to recognize such attacks. Here, it appears that at least two employees with access to the same database provided their credentials in response to common social engineering techniques like phishing.

45. Moreover, cybersecurity experts recommend updating passwords every three months.[12] However, Defendant's public statements about the 2022 Data Incident indicate that the passwords were compromised on or before November 5, 2021, and were not changed, at the earliest, until July 12, 2022.[13] In other words, cybercriminals had unfettered access to the 2022 Plaintiffs' and Class Members' PII for several months longer than would have occurred if Defendant had regularly updated its passwords, regardless of if it had detected a breach.

46. The fact that cybercriminals were able to access the 2022 Plaintiffs' and Class Members' PII with merely compromised passwords also indicates that Defendant failed to implement basic multi-factor authentication on the accounts with compromised passwords and further failed to encrypt PII stored in an internet accessible database while it was not in use.

47. The 2022 Plaintiffs' and Class Members' unencrypted PII has been published on the dark web and will likely end up for sale on the dark web, or simply fall into the hands of

[12] *See* https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/#:~:text=But%20how%20often%20should%20you,has%20access%20to%20your%20account (last visited Apr. 23, 2024).

[13] *See* https://www.uhaul.com/Update/ (last visited Apr. 23, 2024).

companies that will use the detailed PII for targeted marketing without the approval of the 2022 Plaintiffs and Class Members. As a result of the 2022 Data Incident, unauthorized individuals can easily access the PII of the 2022 Plaintiffs and Class Members. Indeed, as detailed below, the exposed PII of the 2022 Plaintiffs and Class Members has already been found on the dark web and misused as a result of the 2022 Data Incident.

48. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for the 2022 Plaintiffs and Class Members, causing the exposure of PII for the 2022 Plaintiffs and Class Members. Specific failures to exercise reasonable care include: failing to encrypt the PII accessed during the 2022 Data Incident; maintaining customer PII for longer than it has a legitimate use; failing to regularly update passwords; failure to implement two-factor authentication for access to accounts and systems containing PII; failing to adequately train employees to recognize phishing and other social engineering techniques; and failing to implement and use software that can adequately detect phishing emails.

The 2023 Data Incident

49. On or about February 22, 2024, Defendant reported the 2023 Data Incident to the Office of the Maine Attorney General and sent Plaintiff Allen and Class Members a letter titled *Notice of Data Breach* (the "Second Notice").[14] Defendant's Second Notice letter informed Plaintiff Allen and other Class Members:

What Happened?

[14] *See Supra* at Footnote No. 5.

> U-Haul learned on December 5, 2023, that legitimate credentials were used by an unauthorized party to access a system U-Haul Dealers and Team Members use to track customer reservations and view customer records. We initiated our response protocol and a cybersecurity firm was engaged to conduct an investigation. The investigation identified specific customer records that were accessed, including one of your records. The information in the record included your name, date of birth and driver's license number. The customer record system that was involved is not a part of our payment system. No payment card data was involved.
>
> **What Information Was Involved?**
>
> The investigation identified certain records that were accessed, and we reviewed those records for personal information. We worked to analyze the customer records involved, and, on December 6, 2023, we determined that your name, date of birth, and drivers license number was accessed by the unauthorized person.
>
> **What We Are Doing?**
>
> We take the privacy of information under our care seriously. To help prevent a similar incident in the future, we have and will continue to take steps to enhance security measures, including changing passwords for affected accounts and implementing additional security safeguards and controls. As a precaution, we are offering you a free one-year membership with Experian IdentityWorksSM Credit 3B. This product helps detect any misuse of your personal information and provides you with identity protection services that focus on immediate identification and resolution of any instance of identity theft. IdentityWorks is completely free to you, and enrolling in this program will not affect your credit score.

50. Defendant admitted in the Notice letter and in their filing with the Office of the Maine Attorney General that an unauthorized actor accessed sensitive information about Plaintiff Allen and Class Members, including their names, dates of birth, and driver's license

numbers or state identification numbers.[15]

51. In the Second Notice letter and in their filing with the Office of the Maine Attorney General Defendant simply states that "[t]o help prevent a similar incident in the future, we have and will continue to take steps to enhance security measures, including changing passwords for affected accounts and implementing additional security safeguards and controls."[16] Notably, Defendant makes no mention of how the credentials used in the 2023 Data Incident were compromised and whether that avenue of attack has been properly identified and addressed.

52. Indeed, Defendant has not provided regulators or Plaintiff Allen and Class Members, who retain a vested interest in ensuring that their information remains protected, any details as to any safeguards or remedial measures undertaken to ensure a breach does not occur again.

53. Other than the statement that the 2023 Data Incident involved "legitimate credentials [] used by an unauthorized party to access [Defendant's] system," and that Defendant secured its systems by changing the passwords of affected accounts more than three months after the 2023 Data Incident was initiated, U-Haul has not shared many details regarding the cause of the 2023 Data Incident. However, the fact that threat actors gained access through stolen legitimate credentials indicates that the 2023 Data Incident was effectuated through phishing or other rudimentary social engineering techniques. Phishing is among the most used

---

[15] *Id.*

[16] *Id.*

methods cybercriminals use to obtain passwords and infiltrate corporate data records. In such an attack, the hacker tricks a legitimate user into inputting their password into a fake website designed to look official. A link to the fake site is often sent by e-mail, with the sender impersonating someone the victim knows and trusts. Defendant could have prevented such an attack by adequately training employees to recognize such attacks. Here, it appears that Defendant's employee(s) with access to the same database provided their credentials in response to common social engineering techniques like phishing.

54. Moreover, cybersecurity experts recommend updating passwords every three months.[17] However, Defendant's public statements about the 2023 Data Incident indicate that the passwords were compromised at an unknown date and were not changed until an unknown time after Defendant learned of the 2023 Data Incident on or about December 5, 2023.[18] In other words, cybercriminals had unfettered access to Plaintiff Allen's and Class Members' PII for an unknown period of time that would not have occurred if Defendant had regularly updated its passwords, regardless of if it had detected a breach.

55. The fact that cybercriminals were able to access Plaintiff Allen's and Class Members' PII with merely compromised passwords also indicates that Defendant failed to implement basic multi-factor authentication on the accounts with compromised passwords and further failed to encrypt PII stored in an internet accessible database while it was not in use.

---

[17] *See* https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/#:~:text=But%20how%20often%20should%20you,has%20access%20to%20your%20account (last visited Apr. 23, 2024).

[18] *See Supra* at Footnote No. 5.

56. Plaintiff Allen's and Class Members' unencrypted PII has been published on the dark web and will likely 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 Allen and Class Members. Indeed, victims of Defendant's prior 2022 Data Incident in or around August of 2022, specifically, Plaintiff Frierson, had their information stolen and posted for sale on the dark web. As a result of the 2023 Data Incident unauthorized individuals can easily access the PII of Plaintiff Allen and Class Members.

57. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff Allen and Class Members, causing the exposure of PII for Plaintiff Allen and Class Members. Specific failures to exercise reasonable care include: failing to encrypt the PII accessed during the 2023 Data Incident; maintaining customer PII for longer than it has a legitimate use; failing to regularly update passwords; failure to implement two-factor authentication for access to accounts and systems containing PII; failing to adequately train employees to recognize phishing and other social engineering techniques; and failing to implement and use software that can adequately detect phishing emails.

Defendant Understood the Risk of a Cyberattack Targeted at the PII of its Customers

58. Because Defendant had a duty to protect Plaintiffs' 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.

59. As evidenced by Defendant already suffering the almost identical 2022 Data

Incident in or around early August of 2022,[19] and Defendant's Privacy Policy and public statements regarding data security, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of the PII maintained by big companies such as Defendant, and (iii) cybercriminals were publishing stolen PII on dark web portals.

60. In light of information readily available and accessible on the Internet before the Data Incidents, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of PII and knew that, due to its public profile, Defendant had cause to be particularly on guard against such an attack.

61. Prior to the Data Incidents, Defendant acknowledged, in its parent company's annual report filed with the SEC in July 2021, as follows:

> 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 man-made 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***

[19] *See Supra* at Footnote No. 5.

> ***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.[20]

62. Prior to the Data Incidents, Defendant knew and understood the foreseeable risk that Plaintiffs' and Class Members' PII could be targeted, accessed, exfiltrated, and published as the result of a cyberattack.

63. Prior to the Data Incidents, Defendant knew or should have known that it should have encrypted the driver's license numbers and other sensitive data elements within the PII it maintained to protect against its publication and misuse in the event of a cyberattack.

64. Prior to the Data Incidents, Defendant knew or should have known that it should

[20] *See* AMERCO 2021 Annual Report, *available at* https://www.amerco.com/reports.aspx (last visited Apr. 23, 2024).

not store sensitive and confidential information in an Internet-accessible environment without necessary encryption, detection, and other basic data security precautions that would have prevented the Data Incidents.

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

66. 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 its electronic records would be targeted by cybercriminals.

67. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued warnings to potential targets so they are aware of, and prepared for, a potential attack. The FBI has warned of phishing attempts designed to gain access to passwords and other credentials for years preceding the Data Incidents.[21] Indeed, as far back as 2018, the FBI published recommendations of basic security measures that companies could employ to prevent and detect phishing schemes, including to:

a. Instruct employees to hover their cursor over hyperlinks included in emails they receive to view the actual URL. Ensure the URL is actually related to or associated with the company it purports to be from.

[21] *See* Cyber Actors Exploit 'Secure' Websites In Phishing Campaigns, available at https://www.ic3.gov/Media/Y2019/PSA190610 (last visited Apr. 23, 2024).

b. Instruct employees to refrain from supplying log-in credentials or personally identifying information in response to any email.
c. Direct employees to forward suspicious requests for personal information to the information technology or human resources department.
d. Ensure that log-in credentials used for payroll purposes differ from those used for other purposes, such as employee surveys.
e. Monitor employee logins that occur outside normal business hours.
f. Restrict access to the Internet on systems handling sensitive information or implement two-factor authentication for access to sensitive systems and information.
g. Only allow required processes to run on systems handling sensitive information.

68. Defendant failed to properly train its employees to detect and report phishing schemes and as a consequence cyberattackers were able to gain access multiple times to unencrypted PII through a relatively simple and common attack vector.

Securing PII and Preventing Breaches

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

70. Defendant could have prevented these Data Incidents by properly securing and encrypting the folders, files, and/or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant should have destroyed the data 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 and with proper safeguards.

71. Several best practices have been identified that at a minimum should be implemented by Defendant, including but not limited to properly training its employees to recognize phishing and other social engineering techniques; employing strong passwords;

regularly updating passwords; implementing multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; and limiting access to sensitive data.

72. Other best cybersecurity practices 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 protecting physical security systems; protecting against any possible communication system; training staff regarding critical points; and increasing the frequency of Penetration Testing.

73. 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.

74. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Incidents.

Defendant Violated the Federal Trade Commission Act

75. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for

business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[23] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

77. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[24]

78. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.
b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
c. Do not store sensitive consumer data on any computer with an Internet connection unless it is essential for conducting their business.
d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, a business should consider closing the ports to those

[22] *See* Federal Trade Commission, *Start With Security*, *available at*: https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Apr. 23, 2024).
[23] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Apr. 23, 2024).
[24] FTC, *Start With Security*, *supra* note 18.

services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the Internet.

g. Determine whether a border firewall should be installed where the business's network connects to the Internet. A border firewall separates the network from the Internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

79. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

80. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. Defendant was at all times fully aware of its obligation to protect the personal and financial data of employees, including Plaintiffs and Class Members. Defendant was also aware of the significant repercussions if it failed to do so.

82. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' PII—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

83. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

Plaintiffs and Class Members Face a Substantial Risk of Imminent Harm

84. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25] 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."[26]

85. 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

[25] 17 C.F.R. § 248.201 (2013).
[26] *Id.*

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.

86. 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 victims.

87. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[27]

88. 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.

---

[27] "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 of 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 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://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited Apr. 23, 2024).

89. The development of "Fullz" packages means here that the stolen PII from the Data Incidents can easily be used to link and identify it to Plaintiffs' 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 Incidents, 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.

90. The existence and prevalence of "Fullz" packages means that the PII stolen from the Data Incidents can easily be linked to the unregulated data of Plaintiffs and the other Class Members. Cybercriminals can then use this information to misrepresent their identity to gain access to financial and other accounts by providing verifying information complied from unique sources.

91. Thus, even if certain information (such as Social Security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

93. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[28] For example, the driver's license and state issued identification information stolen in the Data Incidents can be used to create fake driver's licenses, open accounts in your

[28] *See* "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Apr. 23, 2024) (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

name, avoid traffic tickets or collect government benefits such as unemployment checks.[29] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

94. An individual's full name, date of birth, and driver's license number are, on their own, sufficient for an individual to commit fraud. For example:

> Driver's license fraud specifically occurs when someone uses counterfeit identity documents or another person's identity to obtain a legitimate driver's license or ID card.
>
> This happens when someone is not eligible for a real license. Driver's license fraud is most often committed by an undocumented alien or someone with a suspended or revoked license.
> …
> Slightly different from driver's license fraud, criminals only need your driver's license number (not the whole license) to create a fake ID that they can use instead of their own.
>
> If they have an outstanding warrant and are detained by law enforcement, a cop will run a background check on your ID (which is probably clean) instead of theirs. When the warrant doesn't show up in the background check, the criminals will evade the arrest.
>
> If criminals get stopped for a traffic violation and use your ID, law enforcement will file the charges on your driving record, not theirs. So you'll be on the hook for paying traffic tickets and clearing your name in court.
> …
> Unfortunately, most people don't find out about these unpaid tickets or court appearances until it's too late. A judge will issue a bench warrant for your arrest if you fail to pay these fines or never show up in court.
> …
> Criminals can also use your driver's license to commit synthetic identity theft. These "synthetic" identities combine stolen data from data breaches, your real online footprint, and fake information.

[29] *See* https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Apr. 23, 2024).

> They may use your real driver's license number with a fake name and date of birth. Then they can establish a synthetic identity to run a phishing scam on social media, open new accounts, obtain government documents, and more.
>
> It's nearly impossible to find and stop criminals using a synthetic identity because law enforcement can't determine what's real versus fake. Criminals using synthetic identities are like ghosts in the wind.[30]

95. According to the data privacy and cyber security publication CPO Magazine:

> To 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. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: ". . . 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. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.[31]

96. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application: "Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like

---

[30] *See* https://www.aura.com/learn/can-someone-steal-your-identity-with-your-id (last visited Apr. 23, 2024).

[31] *See* Ikeda, Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims, CPO Magazine (April 23, 2021), available at https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Apr. 23, 2024).

a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name."[32]

97. In some ways, driver's license numbers are even more attractive than Social Security numbers to threat actors and more dangerous to the consumer when compromised. Unlike a Social Security number, a driver's license number isn't monitored as closely, so it can potentially be used in ways that won't immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend that immediate notice, replacement, and identity theft protections are put in place for multiple years.[33]

98. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue

[32] *See* Zach Whittaker, Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months, TechCrunch (Apr. 19, 2021), available at https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/ (last visited Apr. 23, 2024).

[33] *See, e.g.*, https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Apr. 23, 2024).

for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

99. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[35] Victims of the Data Incidents, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Incidents.[36]

100. As a direct and proximate result of the Data Incidents, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Incidents on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account

---

[34] *See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, p. 29, available at https://www.gao.gov/products/gao-07-737 (last visited Apr. 23, 2024).

[35] *See 2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), available at https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Apr. 23, 2024).

[36] *See* "Guide for Assisting Identity Theft Victims," Federal Trade Commission, (Sept. 2013), available at http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited Apr. 23, 2024).

information for unauthorized activity for years to come.

101. Third-party reports about these Data Incidents have specifically warned Plaintiffs and Class Members that:

> Hackers often sell things like stolen driver's licenses and addresses on the dark web. If someone has your license number, they can open up accounts and cards under your name, which can thoroughly ruin your credit score and bank account. Your future, your reputation, and your physical and mental health can all be affected by identity theft.
>
> …
>
> Pay attention to your credit score, manage notifications, and install software designed to protect you. You can find various protectors for your personal information, such as identity monitoring services. They will notify you when your name, social security number, or other self-identifying information is found on sketchy websites. This way, you can spend your time focusing on the beautiful parts of life, not the ones you should be scared of.[37]

102. Other publications have stated that victims of these Data Incidents "could be at a higher risk for fraud or phishing attacks. It is important to stay vigilant moving forward after an incident like this."[38]

103. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including driver's license numbers, 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 Plaintiffs and Class Members as a result of a breach.

104. Plaintiffs and Class Members now face years of constant surveillance of their

[37] *See* https://www.idstrong.com/sentinel/u-haul-data-breach/ (last visited Apr. 23, 2024).

[38] *See* https://www.binarydefense.com/resources/threat-watch/u-haul-customer-data-compromised/ (last visited Apr. 23, 2024).

financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

105. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool and in Defendant's system used by U-Haul Dealers and Team Members to track customer reservations and view customer records, amounting to potentially millions of individuals detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

106. To date, Defendant has offered Plaintiffs and Class Members temporary, non-automatic credit monitoring and identity theft detection through Equifax for the 2022 Data Incident and Experian for the 2023 Data Incident. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. However, Defendant's offers of temporary credit and identity monitoring serves as a tacit recognition by Defendant of the risk that Plaintiffs and Class Members face from the Data Incidents.

107. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including for:

a. Trespass, damage to, and theft of their personal property including PII;

b. Improper disclosure of their PII;

c. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Incidents;

f. Loss of privacy suffered as a result of the Data Incidents;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Incidents;

h. Ascertainable losses in the form of deprivation of the value of their Personal Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

108. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class Members' PII.

109. The injuries to Plaintiffs and Class Members were, and will continue to be, directly and proximately caused by Defendant's failure to implement or maintain adequate data

security measures for the PII of Plaintiffs and Class Members.

Value of Personal Identifiable Information

110. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, stolen driver's license numbers can be sold for between $10 and $35 each.[39] In fact, driver's license numbers are even more valuable than Social Security numbers (which can reportedly be purchased for as little as $1.00).[40]

111. An active and robust legitimate marketplace for PII exists. In 2021, the data brokering industry was worth roughly $200 billion.[41] 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.'[42] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[43] Users of the personal data collection app Streamlytics can earn

---

[39] *See* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Apr. 23, 2024); *see also* https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited Apr. 23, 2024).

[40] *See* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Apr. 23, 2024); *see also* https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited Apr. 23, 2024).

[41] *See* https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Apr. 23, 2024).

[42] *See* https://www.standardbank.co.za/southafrica/personal/products-and-services/security-centre/bank-safely/bank-securely-with-a-digital-id (last visited Apr. 23, 2024).

[43] *See* Nielsen Computer & Mobile Panel, *Frequently Asked Questions,* available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Apr. 23, 2024).

up to $200 a month by selling their personal information to marketing companies who use it to build consumer demographics profiles.[44]

112. Consumers also recognize the value of their personal information, and offer it in exchange for goods and services. The value of PII can be derived not by a price at which consumers themselves actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it. For example, Plaintiffs and Class Members were only to obtain services from Defendant after providing it with their PII. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Similarly, someone with false or negative reports tied to their driver's license may be unable to rent a vehicle or storage unit. In this sense, among others, the theft of PII in the Data Incidents led to a diminution in value of the PII.

113. As a result of the Data Incidents, Plaintiffs' 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 Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

114. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Incidents has been used and will continue to be used

[44] *See* How To Sell Your Own Data And Why You May Want to, available at https://www.mic.com/impact/selling-personal-data-streamlytics (last visited Apr. 23, 2024).

in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

115. The information compromised in the Data Incidents 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 these Data Incidents is impossible to "close" and difficult, if not impossible, to change.

116. These were financially motivated Data Incidents, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against a company like U-Haul is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

117. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[45] For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits. And the personal information of 7 million individuals stolen in a 2021 attack from Luxottica was published online in 2023.[46]

Plaintiff Anderson's Experience

118. Plaintiff Anderson entrusted her Private Information to U-Haul.

---

[45] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737 (last visited Apr. 23, 2024).

[46] *See* https://www.bleepingcomputer.com/news/security/luxottica-confirms-2021-data-breach-after-info-of-70m-leaks-online/ (last visited Apr. 23, 2024).

119. Plaintiff Anderson and Class Members were required to provide their Private Information, including a copy of their driver's license, to U-Haul in order to receive vehicle or storage rental services.

120. Plaintiff Anderson and Class Members entrusted their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiff Anderson would not have allowed U-Haul to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

121. On September 9, 2022, Plaintiff Anderson received an email from Defendant, informing her that her Private Information, including her name and driver's license number, was identified as having been accessed by cybercriminals during the 2022 Data Incident.

122. Because of the 2022 Data Incident, Plaintiff Anderson's Private Information is now in the hands of cybercriminals. Plaintiff Anderson and all Class Members are imminently at risk of future identity theft and fraud.

123. As a result of the 2022 Data Incident, Plaintiff Anderson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the 2022 Data Incident. Specifically, Plaintiff Anderson has devoted time to, among other things, investigating the 2022 Data Incident, reviewing account statements and other personal information, contacting her credit card company in response to the fraudulent charges, and working to establish different payment methods for the accounts that were being automatically billed to the closed account.

124. Plaintiff Anderson anticipates spending additional time and money on an ongoing

basis to try to mitigate and address harms caused by the 2022 Data Incident. In addition, Plaintiff Anderson will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

125. In fact, Plaintiff Anderson has already experienced identity fraud and data misuse. Plaintiff Anderson has recently become aware of fraudulent charges on her credit card since the time of the 2022 Data Incident. In response, Plaintiff Anderson had to devote time to closing her credit card that was used and get a new card issued. This has involved considerable time for Plaintiff Anderson, as she used to have all bills automatically taken out of her account. It is unlikely that this fraud stemmed from other incidents because prior to the 2022 Data Incident, Plaintiff Anderson exercised reasonable care in keeping her sensitive data, including driver's license number and financial account information, private and secure. For example, Plaintiff Anderson has never knowingly transmitted Private Information, including her driver's license number and financial account information, over the internet in an unencrypted or other insecure manner. Moreover, Plaintiff Anderson keeps any documents with her Private Information, including driver's license number and financial account information, in a safe and secure place, or destroys such documents if they are no longer needed. To the best of Plaintiff Anderson's knowledge, she has never been the victim of another data breach.

126. Plaintiff Anderson has suffered injury directly and proximately caused by the 2022 Data Incident, including: (a) theft of Plaintiff Anderson's valuable Private Information; (b) identity theft and data misuse in the form of fraudulent charges; (c) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Anderson's Private Information being placed in the hands of cyber criminals; (d) damages to and diminution in

value of Plaintiff Anderson's Private Information that was entrusted to Defendant for the sole purpose of obtaining rental or storage services with the understanding that Defendant would safeguard this information against disclosure; (e) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Anderson should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Anderson's Private Information; (f) invasion of her privacy; and (g) continued risk to Plaintiff Anderson's Private Information, 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 the Private Information that was entrusted to Defendant.

Plaintiff Hendricks's Experience

127. Plaintiff Hendricks entrusted her Private Information to U-Haul.

128. Plaintiff Hendricks and Class Members were required to provide their Private Information, including a copy of their driver's license, to U-Haul in order to receive vehicle or storage rental services.

129. Plaintiff Hendricks and Class Members entrusted their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiff Hendricks would not have allowed U-Haul to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

130. On September 9, 2022, Plaintiff Hendricks received an email from Defendant,

informing him that her Private Information, including her name and driver's license number, was identified as having been accessed by cybercriminals during the 2022 Data Incident.

131. Because of the 2022 Data Incident, Plaintiff Hendricks's Private Information is now in the hands of cybercriminals. Plaintiff Hendricks and all Class Members are imminently at risk of future identity theft and fraud.

132. As a result of the 2022 Data Incident, Plaintiff Hendricks has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the 2022 Data Incident. Specifically, Plaintiff Hendricks has devoted time to, among other things, investigating the 2022 Data Incident, reviewing account statements and other personal information, and taking other steps in response to the 2022 Data Incident.

133. Plaintiff Hendricks anticipates spending additional time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. In addition, Plaintiff Hendricks will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

134. Plaintiff Hendricks has suffered injury directly and proximately caused by the 2022 Data Incident, including: (a) theft of Plaintiff Hendricks's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Hendricks's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Hendricks's Private Information that was entrusted to Defendant for the sole purpose of obtaining rental or storage services with the understanding that Defendant would safeguard this information against disclosure; (d) loss of

the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Hendricks should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Hendricks's Private Information; (e) invasion of her privacy; and (f) continued risk to Plaintiff Hendricks's Private Information, 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 the Private Information that was entrusted to Defendant.

Plaintiff Telford's Experience

135. Plaintiff Telford entrusted his Private Information to U-Haul.

136. Plaintiff Telford and Class Members were required to provide their Private Information, including a copy of their driver's license, to U-Haul in order to receive vehicle or storage rental services.

137. Plaintiff Telford and Class Members entrusted their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiff Telford would not have allowed U-Haul to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

138. On September 9, 2022, Plaintiff Telford received an email from Defendant, informing him that his Private Information, including his name and driver's license number, was identified as having been accessed by cybercriminals during the 2022 Data Incident.

139. Because of the 2022 Data Incident, Plaintiff Telford's Private Information is now

in the hands of cybercriminals. Plaintiff Telford and all Class Members are imminently at risk of future identity theft and fraud.

140. As a result of the 2022 Data Incident, Plaintiff Telford has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the 2022 Data Incident. Specifically, Plaintiff Telford has devoted time to, among other things, investigating the 2022 Data Incident, reviewing account statements, signing up for identity theft protection services, and checking other personal information on a near daily basis. As a result of the 2022 Data Incident, Plaintiff Telford also lost personal funds to pay for gas to the nearest U-Haul location.

141. Plaintiff Telford anticipates spending additional time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. In addition, Plaintiff Telford will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

142. Plaintiff Telford has suffered injury directly and proximately caused by the 2022 Data Incident, including: (a) theft of Plaintiff Telford's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Telford's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Telford's Private Information that was entrusted to Defendant for the sole purpose of obtaining rental or storage services with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Telford should have received from Defendant and Defendant's

defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Telford's Private Information; (e) invasion of his privacy; and (f) continued risk to Plaintiff Telford's Private Information, 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 the Private Information that was entrusted to Defendant.

Plaintiff Rolon's Experience

143. Plaintiff Rolon was required to provide and did provide his PII to Defendant.

144. The PII included his name and driver's license or state identification number.

145. To date, U-Haul has done next to nothing to adequately protect Plaintiff Rolon and Class Members, or to compensate them for their injuries sustained in the 2022 Data Incident, offering only an optional subscription to Equifax's Identity Theft Protection program.

146. Defendant's 2022 Data Incident Notice letter downplays the theft of Plaintiffs' 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 Rolon 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.

147. Plaintiffs and Class Members have been further damaged by the compromise of their PII.

148. Plaintiff Rolon's PII was compromised in the 2022 Data Incident 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.

149. Plaintiff Rolon 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.

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

151. As a result of the 2022 Data Incident, Plaintiff Rolon 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.

152. As a result of the 2022 Data Incident, Plaintiff Rolon has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to the 2022 Data Incident. 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.

153. Since the 2022 Data Incident, Plaintiff Rolon has also experienced a substantial increase in spam calls, texts, and emails.

154. Plaintiff Rolon 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 2022 Data Incident.

155. Plaintiff Rolon suffered lost time, annoyance, interference, and inconvenience as a result of the 2022 Data Incident and has anxiety and increased concerns for the loss of his

privacy.

156. Plaintiff Rolon 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.

157. Defendant obtained and continues to maintain Plaintiff Rolon'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 Rolon when he received services from Defendant. Plaintiff Rolon, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Rolon's PII was compromised and disclosed as a result of the 2022 Data Incident.

158. As a result of the 2022 Data Incident, Plaintiff Rolon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. As a result of the 2022 Data Incident, Plaintiff Rolon is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Denise Bowen's Experience

159. Plaintiff Denise Bowen was required to provide and did provide her PII to Defendant.

160. The PII included her name and driver's license or state identification number.

161. To date, U-Haul has done next to nothing to adequately protect Plaintiff Denise Bowen and Class Members, or to compensate them for their injuries sustained in the 2022 Data Incident, offering only an optional subscription to Equifax's Identity Theft Protection program.

162. Defendant's Data Breach Notice letter for the 2022 Data Incident downplays the theft of Plaintiffs' 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 Denise Bowen 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.

163. Plaintiffs and Class Members have been further damaged by the compromise of their PII.

164. Plaintiff Denise Bowen's PII was compromised in the 2022 Data Incident and likely stolen and in the hands of cybercriminals who illegally accessed U-Haul International's network for the specific purpose of targeting the PII.

165. Plaintiff Denise Bowen typically takes measures to protect her PII and is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

166. Plaintiff Denise Bowen stores any documents containing her PII in a safe and secure location. And she diligently chooses unique usernames and passwords for her online accounts.

167. As a result of the 2022 Data Incident, Plaintiff Denise Bowen has diligently monitored her credit and financial accounts, while constantly worrying about what her PII could be used for in the future by any third-party with access to the dark web.

168. As a result of the 2022 Data Incident, Plaintiff Denise Bowen has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to the 2022 Data Incident. She 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.

169. Since the 2022 Data Incident, Plaintiff Denise Bowen has also experienced an increase in spam calls, texts, and emails.

170. Plaintiff Denise Bowen also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the 2022 Data Incident.

171. Plaintiff Denise Bowen suffered lost time, annoyance, interference, and inconvenience as a result of the 2022 Data Incident and has anxiety and increased concerns for the loss of her privacy.

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

173. Defendant obtained and continues to maintain Plaintiff Denise Bowen'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 Denise Bowen when she received services from Defendant. Plaintiff Denise Bowen, however, would not have entrusted her PII to

Defendant had she known that it would fail to maintain adequate data security. Plaintiff Denise Bowen's PII was compromised and disclosed as a result of the 2022 Data Incident.

174. As a result of the 2022 Data Incident, Plaintiff Denise Bowen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. As a result of the 2022 Data Incident, Plaintiff Bowen is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Bryan Bowen's Experience

175. Plaintiff Bryan Bowen was required to provide and did provide his PII to Defendant.

176. The PII included his name and driver's license or state identification number.

177. To date, U-Haul has done next to nothing to adequately protect Plaintiff Bryan Bowen and Class Members, or to compensate them for their injuries sustained in the 2022 Data Incident, offering only an optional subscription to Equifax's Identity Theft Protection program.

178. Defendant's data breach notice letter for the 2022 Data Incident downplays the theft of Plaintiffs' 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 Plaintiffs 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.

179. Plaintiffs and Class Members have been further damaged by the compromise of their PII.

180. Plaintiff Bryan Bowen's PII was compromised in the 2022 Data Incident 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.

181. Plaintiff Bryan Bowen 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.

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

183. As a result of the 2022 Data Incident, Plaintiff Bryan Bowen 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.

184. As a result of the 2022 Data Incident, Plaintiff Bryan Bowen has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to the 2022 Data Incident. 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.

185. Since the 2022 Data Incident, Plaintiff Bryan Bowen has also experienced a substantial increase in spam calls, texts, and emails.

186. Plaintiff Bryan Bowen 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 2022 Data Incident.

187. Plaintiff Bryan Bowen suffered lost time, annoyance, interference, and inconvenience as a result of the 2022 Data Incident and has anxiety and increased concerns for the loss of his privacy.

188. 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.

189. Defendant obtained and continues to maintain Plaintiff Bryan Bowen'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 Bryan Bowen, 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 2022 Data Incident.

190. As a result of the 2022 Data Incident, Plaintiff Bryan Bowen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. As a result of the 2022 Data Incident, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Johnson's Experience

191. Plaintiff Johnson was required to provide and did provide his PII to Defendant.

192. The PII included his name and driver's license or state identification number.

193. To date, U-Haul has done next to nothing to adequately protect Plaintiff Johnson and Class Members, or to compensate them for their injuries sustained in the 2022 Data Incident, offering only an optional subscription to Equifax's Identity Theft Protection program.

194. Defendant's data breach notice letter for the 2022 Data Incident downplays the theft of Plaintiffs' 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 Plaintiffs 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.

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

196. Plaintiff Johnson's PII was compromised in the 2022 Data Incident 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.

197. Plaintiff Johnson 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.

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

199. As a result of the 2022 Data Incident, 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.

200. As a result of the 2022 Data Incident, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to the 2022 Data Incident, including, but researching the verifying the legitimacy of the 2022 Data Incident, signing up for the credit monitoring and identity theft protection services offered by Defendant, securing his credit accounts, monitoring his financial accounts for unusual activity. This is time that was lost and unproductive and took away from other activities and duties. Moreover, he has sustained emotional distress.

201. Since the 2022 Data Incident, Plaintiff has also experienced a substantial increase in spam calls, texts, and emails.

202. Plaintiff Johnson 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 2022 Data Incident.

203. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the 2022 Data Incident and has anxiety and increased concerns for the loss of his privacy.

204. 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.

205. Defendant obtained and continues to maintain Plaintiff Johnson'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 2022 Data Incident.

206. As a result of the 2022 Data Incident, Plaintiff Johnson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. As a result of the 2022 Data Incident, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Rivera's Experience

207. Plaintiff Rivera was required to provide and did provide his PII to Defendant.

208. The PII included his name and driver's license or state identification number.

209. To date, U-Haul has done next to nothing to adequately protect Plaintiff Rolon and Class Members, or to compensate them for their injuries sustained in the 2022 Data Incident, offering only an optional subscription to Equifax's Identity Theft Protection program.

210. Defendant's data breach notice letter for the 2022 Data Incident downplays the theft of Plaintiffs' 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 Plaintiffs 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.

211. Plaintiffs and Class Members have been further damaged by the compromise of their PII.

212. Plaintiff Rivera's PII was compromised in the 2022 Data Incident 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.

213. Plaintiff Rivera 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.

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

215. As a result of the 2022 Data Incident, 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.

216. As a result of the 2022 Data Incident, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to the 2022 Data Incident. 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.

217. Since the 2022 Data Incident, Plaintiff has also experienced a substantial increase in spam calls, texts, and emails.

218. Plaintiff Rivera 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 2022 Data Incident.

219. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the 2022 Data Incident and has anxiety and increased concerns for the loss of his privacy.

220. 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.

221. Defendant obtained and continues to maintain Plaintiff Rivera'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 2022 Data Incident.

222. As a result of the 2022 Data Incident, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the 2022 Data Incident. As a result of the 2022 Data Incident, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Allen's Experience

223. Plaintiff Ariana Allen entrusted her Private Information to U-Haul.

224. Plaintiff Allen and Class Members were required to provide their Private Information, including a copy of their driver's license, phone number, and email to U-Haul in order to receive vehicle or storage rental services.

225. Plaintiff Allen and Class Members entrusted their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would

comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiff Allen would not have allowed U-Haul to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

226. On February 22, 2024, Plaintiff Allen received a Notice of Data Breach letter for the 2023 Data Incident from Defendant, informing her that her Private Information, including her name, date of birth, and driver's license number, was identified as having been accessed by cybercriminals during the 2023 Data Incident.

227. Because of the 2023 Data Incident, Plaintiff Allen's Private Information is now in the hands of cybercriminals. Plaintiff Allen and all Class Members are imminently at risk of future identity theft and fraud.

228. After the 2023 Data Incident occurred, Plaintiff Allen suffered an unauthorized third-party attempting to access her PayPal account and change her login information and password. Plaintiff Allen has also suffered a substantial increase in spam calls, emails, and texts as a result of the 2023 Data Incident.

229. As a result of the 2023 Data Incident, Plaintiff Allen has already expended approximately 4 hours of time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the 2023 Data Incident. Specifically, Plaintiff Allen has devoted time to, among other things, investigating the 2023 Data Incident, reviewing account statements, signing up for identity theft protection services, and checking other personal information on a near daily basis. As a result of the 2023 Data Incident, Plaintiff Allen also lost personal funds to pay for gas to her bank to discuss the implications of the 2023 Data Incident.

230. Plaintiff Allen anticipates spending additional time and money on an ongoing basis to try to mitigate and address harms caused by the 2023 Data Incident. In addition, Plaintiff Allen will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

231. Plaintiff Allen has suffered injury directly and proximately caused by the 2023 Data Incident, including: (a) theft of Plaintiff Allen's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Allen's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Allen's Private Information that was entrusted to Defendant for the sole purpose of obtaining rental or storage services with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Allen should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Allen's Private Information; (e) invasion of her privacy; and (f) continued risk to Plaintiff Allen's Private Information, 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 the Private Information that was entrusted to Defendant.

V. CLASS ALLEGATIONS

232. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

233. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals who resided in California at any time during, and whose PII was compromised in, the 2022 and/or 2023 Data Incidents that are the subjects of the *Notice of Recent Security Incident* or *Notice of Data Breach* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 and February 22, 2024, respectively (the "Class").

234. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

235. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

236. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable with the Settlement Class totally roughly 259,000 individuals. Defendant has identified numerous individuals whose PII was compromised in the Data Incidents, and the Class Members are apparently identifiable within Defendant's records.

237. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact are common to the Class Members and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Incidents;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. 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 Incidents;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Incidents to occur;

j. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or

nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Incidents.

238. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Incidents, due to Defendant's misfeasance.

239. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

240. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

241. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

242. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

243. The litigation of the claims brought herein is manageable. Defendant's uniform

conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

244. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

245. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Incidents, and Defendant may continue to act unlawfully as set forth in this complaint.

246. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws,

regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

e. 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 Incidents; and,

f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Violations of California's Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On behalf of Plaintiffs and the Class)

248. Plaintiffs re-allege and incorporate by reference paragraphs 1-231 as if fully set forth herein.

249. Plaintiffs bring this Count on their own behalf and on behalf of the Class.

250. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[47]

[47] *See* California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/ (last visited March 13, 2024).

251. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Incidents.

252. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

253. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

254. Plaintiffs and Class Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

255. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

256. The Private Information taken in the Data Incidents is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and Class Members' unencrypted first and last names and driver's licenses among other information.

257. Plaintiffs' and Class Members' unencrypted and unredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

258. The Data Incidents occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and Class Members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its server or network, including its email, customer tracking, and customer record keeping systems, by hackers and to prevent unauthorized access of Plaintiffs' and Class Members' PII as a result of these attacks.

259. Plaintiffs Anderson, Hendricks, Telford, Rolon, Denise Bowen, Bryan Bowen, Johnson, and Rivera each provided Defendant with written notice of Defendant's violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant has not responded to these written notices and has not cured or is unable to cure the violations described herein. Plaintiffs seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount between one hundred ($100) and seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

260. On March 1, 2024, Plaintiff Allen provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant fails to respond, or has not cured, or is unable to cure the violation within 30 days thereof, she will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

261. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Incidents, in addition to actual or statutory

damages, Plaintiffs seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and their Counsel to represent such Class;

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

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

v. prohibiting Defendant from maintaining the PII of Plaintiffs 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 Plaintiffs 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 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;

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 personal identifying information 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;

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: May 8, 2024.

Respectfully Submitted,

/s/ Cristina Perez Hesano
PEREZ LAW GROUP, PLLC
Cristina Perez Hesano (#027023)
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: (602) 730-7100

Facsimile: (623) 235-6173
Email: *cperez@perezlawgroup.com*

Terence R. Coates*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
Email: *tcoates@msdlegal.com*

M. Anderson Berry*
Gregory Haroutunian*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
Emails: *aberry@justice4you.com*
gharoutunian@justice4you.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Email: *gklinger@milberg.com*

Rory Brian Riley (ASB 03293)
Morgan and Morgan Arizona PLLC
2355 E. Camelback Road Suite 335
Phoenix, AZ 85016
Telephone: (602) 735-0250
Email: *briley@forthepeople.com*

John A. Yanchunis*
MORGAN & MORGAN COMPLEX
BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602

Telephone: (813) 223-5505
Emails: *jyanchunis@ForThePeople.com*

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: *wbf@federmanlaw.com*
-and-
212 W. Spring Valley Road
Richardson, Texas 75081

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
Email: *abm@murphylegalfirm.com*

Mark S. Reich*
Courtney E. Maccarone*
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, NY 10006
Telephone: 212-363-7500
Facsimile: 212-363-7171
Emails: *mreich@zlk.com*
cmaccarone@zlk.com

Paul L. Stoller (No. 016773)
Jennifer Rethemeier (No. 031398)
DALIMONTE RUEB STOLLER, LLP
2425 E. Camelback Road, Suite 500
Phoenix, Arizona 85016
Telephone: (602) 892-0341
Facsimile: (855) 203-2035
Emails: *jennifer.rethemeier@drlawllp.com*
paul@drlawllp.com

Marc E. Dann*
Brian D. Flick*

DANNLAW
15000 Madison Avenue
Lakewood, OH 44107
Emails: *mdann@dannlaw.com*
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Telephone: (312) 440-0020
Emails: *tom@attorneyzim.com*
firm@attorneyzim.com

Robert D. Mitchell
Christopher J. Waznik
Anne P. Barber CM
Matthew Luk
TIFFANY & BOSCO P.A.
Camelback Esplanade II, Seventh Floor
2525 East Camelback Road
Phoenix, Arizona 85016
Emails: *rdm@tblaw.com*
cjw@tblaw.com
apb@tblaw.com
cml@tblaw.com

Marcus J. Bradley*
Kiley L. Grombacher*
BRADLEY/GROMBACHER, LLP
31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
Emails: *mbradley@bradleygrombacher.com*
kgrombacher@bradleygrombacher.com

Attorneys for Plaintiffs and the Proposed Class

*admitted *pro hac vice*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 8th day of May, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail notice list.

/s/ *Cristina Perez Hesano*
Cristina Perez Hesano (#027023)