Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100
Fax: 623.235.6173

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

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Felicia Durgan; William Frierson; Michelle Anderson; Saray Hendricks; Shawnda Lauderdale; Amy Dobson; Delbert Gibson III; Bruce Proctor Jr.; and Peter Telford; 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. **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Felicia Durgan, William Frierson, Michelle Anderson, Saray Hendricks, Shawnda Lauderdale, Amy Dobson, Delbert Gibson III, Bruce Proctor Jr., and Peter Telford ("Plaintiffs") bring this 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 "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 April 5, 2022, Defendant obtained the PII of Plaintiffs and Class Members, including the PII of Plaintiffs, who were customers of Defendant, and stored that PII unencrypted and in an Internet-accessible environment on Defendant's network.

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:

"[w]e use commercially reasonable physical, managerial, and technical

---

[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 Sept. 12, 2022).

[3] *See* https://finance.yahoo.com/news/uhal-amerco-crosses-4-billion-092300411.html (last visited Dec. 13, 2022).

> safeguards to preserve the integrity and security of your Information and our systems. We cannot, however, ensure or warrant the security of any information you transmit to Us and you do so at your own risk. However, please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards."[4]

6. Despite this, on July 12, 2022, Defendant learned of a data security 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 Plaintiffs and Class Members (the "Data Breach").

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

8. On or around September 9, 2022, nearly two months after discovering the Data Breach, Defendant began notifying Plaintiffs and Class Members that their PII had been compromised in the Data Breach.

9. 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.

10. The exposed PII of Plaintiffs and Class Members will likely be sold on the dark

[4] *See* https://www.uhaul.com/Legal/PrivacyPolicy/#Security (last visited Dec. 13, 2022).

web. Hackers target companies like Defendant to access and then offer for sale the unencrypted, unredacted PII they maintain to other criminals. Plaintiffs and Class Members now face an ongoing and lifetime risk of identity theft, which is heightened here by the loss of driver's license numbers or state identification numbers in conjunction with verifying information like the names and dates of birth of Plaintiffs and Class Members.

11. 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 Data Breach occurred to report it to the SEC and affected individuals which prevented them from taking efforts to timely mitigate the consequences of the Data Breach.

12. 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.

13. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiffs and Class Members of the Data Breach. Defendant's conduct amounts at least to

negligence and violates federal and state statutes.

14. 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 Breach, 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.

15. 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 the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. 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

16. Plaintiff Felicia Durgan is a citizen of Virginia residing in Stafford, Virginia.

17. Plaintiff William Frierson is a citizen of Arizona residing in Chandler, Arizona.

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 Shawnda Lauderdale is a citizen of Indiana residing in South Bend, Indiana.

21. Plaintiff Amy Dobson is a citizen of New York residing in Syracuse, New York.

22. Plaintiff Delbert Gibson III is a citizen of Oregon residing in Myrtle Creek, Oregon.

23. Plaintiff Bruce Proctor, Jr. is a citizen of Pennsylvania residing in Pittsburgh, Pennsylvania.

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

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

26. 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.

27. 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

28. 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.

29. 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.

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

31. 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

Background

32. 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.

33. 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.

34. 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 Data Breach

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

36. Defendant also filed a notice with the SEC advising that the compromised PII included names, dates of birth, and driver's license numbers.[5]

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

38. In response to the Data Breach, Defendant claimed that cybersecurity experts "are implementing additional security safeguards and controls to prevent further such incidents."[6] 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 Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

39. The unencrypted PII of Plaintiffs and Class Members 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

[5] *See* Exhibit 1.
[6] *Id*.

targeted marketing without the approval of Plaintiffs and Class Members. As a result of the Data Breach unauthorized individuals can easily access the PII of Plaintiffs and Class Members. Indeed, as detailed below, the exposed PII of Plaintiffs and Class Members has already been misused as a result of the Data Breach.

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

41. 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.

42. As evidenced by 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 big companies such as Defendant, and (iii) cybercriminals were publishing stolen PII on dark web portals.

43. In light of information readily available and accessible on the Internet before the Data Breach, 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.

44. Prior to the Data Breach, 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 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.[7]

[7] AMERCO 2021 Annual Report, *available at* https://www.amerco.com/reports.aspx (last visited Dec. 13, 2022). AMERCO is the parent company of Defendant.

45. Prior to the Data Breach, 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.

46. Prior to the Data Breach, 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.

47. Prior to the Data Breach, Defendant knew or should have known that it should 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 this Data Breach.

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

48. As a condition of receiving services from Defendant, Defendant required that Plaintiffs and Class Members entrust Defendant with highly confidential PII. Plaintiff and Class Members provided their PII on the condition and with the expectation that it be maintained as confidential and safeguarded against unauthorized access.

49. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members and used it 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.

50. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was

responsible for protecting the PII from disclosure.

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

Securing PII and Preventing Breaches

52. 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.

53. 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.

54. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

55. 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.

56. Defendant could have prevented this Data Breach 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.

57. Several best practices have been identified that at a minimum should be implemented by Defendant, including but not limited to employing; strong passwords; 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.

58. 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.

59. 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.

60. 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 Breach.

61. 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.[8]

62. 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.[9] 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.

63. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[10]

64. 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

[8] Federal Trade Commission, *Start With Security*, *available at*: https://www.ftc.gov/system/files /documents/plain-language/pdf0205-startwithsecurity.pdf.
[9] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide- business.
[10] FTC, *Start With Security*, *supra* note 18.

connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

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

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

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

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

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

65. 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.

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

67. 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.

68. 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.

69. 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.

Value of Personal Identifiable Information

70. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] 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."[12]

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*

71. 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, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

72. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

73. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[15] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 13, 2022).

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 13, 2022).

[15] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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." 12 C.F.R. § 1022.3(g).

bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[16]

74. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

75. 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.

76. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[17] For example, the driver's license and state issued identification information stolen in the Data Breach can be used to create fake driver's licenses, open accounts in your

---

[16] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited December 13, 2022).

[17] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (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.[18] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

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

78. This was a financially motivated Data Breach, 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. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market." [19]

79. 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

[18] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[19] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 13, 2022).

years.[20] 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.

80. 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 for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

81. 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.[22] Victims of the Data Breach, 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 Breach.[23]

82. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of

---

[20] *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/assets/270/262904.htmlu

[21] *Data Breaches Are Frequent*, *supra* note 11.

[22] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited December 13, 2022).

[23] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013 http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

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 Breach 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 information for unauthorized activity for years to come.

83. 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.

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

85. 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, 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.

86. To date, Defendant has offered Plaintiffs and Class Members only one year of credit monitoring and identity theft detection through Equifax. The offered service is 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.

87. 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 Breach;

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

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 Breach;

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.

88. 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.

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

Plaintiff Durgan's Experience

90. Plaintiff Durgan entrusted her Private Information to U-Haul.

91. Plaintiff Durgan 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.

92. Plaintiff Durgan 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 Durgan would not have allowed U-Haul to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

93. On September 9, 2022, Plaintiff Durgan received an email from Defendant, informing her that her Private Information, including her name and driver's license or state

identification number, was identified as having been accessed by cybercriminals during the Data Breach.

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

95. As a result of the Data Breach, Plaintiff Durgan 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 Data Breach. Specifically, Plaintiff Durgan has devoted time to, among other things, investigating the Data Breach, researching how best to ensure that she is protected from identity theft, changing passwords, and reviewing account statements and other information.

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

97. Plaintiff Durgan has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Durgan's valuable Private Information; (b) identity theft and data misuse in the form of her Social Security number being compromised and found on the dark web; (c) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Durgan's Private Information being placed in the hands of cyber criminals; (d) damages to and diminution in value of Plaintiff Durgan'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 Durgan 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 Durgan's Private Information; and (f) continued risk to Plaintiff Durgan'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 Frierson's Experience

98. Plaintiff Frierson entrusted his Private Information to U-Haul.

99. Plaintiff Frierson 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.

100. Plaintiff Frierson 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 Frierson would not have allowed U-Haul to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

101. On September 9, 2022, Plaintiff Frierson 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 Data Breach.

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

103. As a result of the Data Breach, Plaintiff Frierson 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 Data Breach. Specifically, Plaintiff has devoted time to, among other things, investigating the Data Breach, researching how best to ensure that he is protected from identity theft, changing passwords, and reviewing account statements and other information.

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

105. In fact, Plaintiff Frierson has already experienced identity fraud and data misuse. In November 2022, Plaintiff Frierson noticed a fraudulent charge on his banking account. A few days later, Plaintiff Frierson was locked out of his account because someone was trying to access his online banking information. As a result of the foregoing, Plaintiff Frierson was unable to access the funds in his bank account for multiple days and had to notify his bank of the issues. Plaintiff Frierson also recently received a notification from Experian that his information was located on the dark web.

106. Plaintiff Frierson has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Frierson's valuable Private Information; (b) identity

theft and data misuse in the form of fraudulent charges and a notification that his information has been posted on the dark web; (c) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Frierson's Private Information being placed in the hands of cyber criminals; (d) damages to and diminution in value of Plaintiff Frierson'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 Frierson 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 Frierson's Private Information; and (f) continued risk to Plaintiff Frierson'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 Anderson's Experience

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

108. 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.

109. 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.

110. 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 Data Breach.

111. Because of the Data Breach, 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.

112. As a result of the Data Breach, 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 Data Breach. Specifically, Plaintiff Anderson has devoted time to, among other things, investigating the Data Breach, 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.

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

114. 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 Data Breach. 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.

115. Plaintiff Anderson has suffered injury directly and proximately caused by the Data Breach, 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; and (f) 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 Hendrick's Experience

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

117. 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.

118. 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.

119. 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 Data Breach.

120. Because of the Data Breach, 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.

121. As a result of the Data Breach, 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 Data Breach. Specifically, Plaintiff Hendricks has devoted time to, among other things, investigating the Data Breach, reviewing account statements and other personal information, and taking other steps in response to the Data Breach.

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

123. Plaintiff Hendricks has suffered injury directly and proximately caused by the Data Breach, 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; and (e) 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 Lauderdale's Experience

124. Plaintiff Lauderdale entrusted her Private Information to U-Haul.

125. Plaintiff Lauderdale 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. Plaintiff Lauderdale allowed U-Haul to scan her driver's license at the U-Haul facility where she engaged U-Haul's services.

126. Plaintiff Lauderdale 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 Lauderdale would not have allowed U-Haul to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

127. On or about September 9, 2022, Plaintiff Lauderdale 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 Data Breach.

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

129. As a result of the Data Breach, Plaintiff Lauderdale 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 Data Breach. Specifically, Plaintiff Lauderdale has devoted time to, among other things, investigating the Data Breach, researching how best to ensure that she is protected from identity theft, contacting and retaining Credit Karma premium to provide her with credit monitoring services, communicating with her bank regarding fraudulent charges, and reviewing account statements and other information.

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

131. In fact, Plaintiff Lauderdale has already experienced identity fraud and data

misuse. In or around March 2022, Plaintiff Lauderdale noticed fraudulent charges on her debit card. As a result of the foregoing, Plaintiff Lauderdale had to spend time communicating with her bank identifying this charge as fraudulent and getting the bank to reverse the charge.

132. Plaintiff Lauderdale has experienced actual losses as a result of the Data Breach as well. Specifically, following the fraudulent charges on her debit card, Plaintiff Lauderdale had to purchase credit monitoring services from Credit Karma in order to protect her identity and credit from further misuse and identity fraud.

133. Plaintiff Lauderdale has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Lauderdale'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 Lauderdale's Private Information being placed in the hands of cyber criminals; (d) damages to and diminution in value of Plaintiff Lauderdale'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 Lauderdale 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 Lauderdale's Private Information; and (f) continued risk to Plaintiff Lauderdale'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 Proctor's Experience

134. Plaintiff Proctor entrusted his Private Information to U-Haul.

135. Plaintiff Proctor 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.

136. Plaintiff Proctor 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 Proctor would not have allowed U-Haul to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

137. On September 11, 2022, Plaintiff Proctor received an email from Defendant, informing him that his Private Information, including his name and driver's license or state identification number, was identified as having been accessed by cybercriminals during the Data Breach.

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

139. As a result of the Data Breach, Plaintiff Proctor 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 Data Breach. Specifically, Plaintiff Proctor has devoted time to, among other things, investigating the Data Breach, researching how best to

ensure that he is protected from identity theft, changing passwords, and reviewing account statements and other information.

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

141. Plaintiff Proctor suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Proctor's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Proctor's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Proctor'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 Proctor 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 Proctor's Private Information; and (e) continued risk to Plaintiff Proctor'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 Dobson's Experience

142. Plaintiff Dobson entrusted her Private Information to U-Haul.

143. Plaintiff Dobson 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. Plaintiff Dobson allowed U-Haul to scan her driver's license at the U-Haul facility where she engaged U-Haul's services.

144. Plaintiff Dobson 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 Dobson would not have allowed U-Haul to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

145. On or about September 9, 2022, Plaintiff 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 Data Breach.

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

147. As a result of the Data Breach, Plaintiff Dobson 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 Data Breach. Specifically, Plaintiff Dobson has devoted time to, among other things, investigating the Data Breach, researching how best to ensure that she is protected from identity theft, communicating with her bank regarding fraudulent charges she has experienced as a result of the Data Breach, and reviewing account statements and other information.

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

149. In fact, Plaintiff Dobson has already experienced identity fraud and data misuse. At some point after November 2021, Plaintiff Dobson noticed a fraudulent charge on her banking account, from a resort/hotel that she did not stay at or engage in any other way. As a result of the foregoing, Plaintiff Dobson had to spend time communicating with her bank identifying this charge as fraudulent and getting the bank to reverse the charge.

150. Plaintiff Dobson has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Dobson'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 Dobson's Private Information being placed in the hands of cyber criminals; (d) damages to and diminution in value of Plaintiff Dobson'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 Dobson 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 Dobson's Private Information; and (f) continued risk to Plaintiff Dobson'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 Gibson's Experience

151. Plaintiff Gibson entrusted his Private Information to U-Haul.

152. Plaintiff Gibson 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.

153. Plaintiff Gibson 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 Gibson would not have allowed U-Haul to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

154. On September 9, 2022, Plaintiff Gibson 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 Data Breach.

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

156. As a result of the Data Breach, Plaintiff Gibson 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 Data Breach. Specifically, Plaintiff Gibson has devoted time to, among other things, investigating the Data Breach, reviewing account

statements, checking credit reports, and going to U-Haul to ask questions about the Data Breach. As a result of the Data Breach, Plaintiff Gibson also lost personal funds to pay for gas to the nearest U-Haul location.

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

158. Plaintiff Gibson has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Gibson's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Gibson's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Gibson'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 Gibson 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 Gibson's Private Information; and (e) continued risk to Plaintiff Gibson'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

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

160. 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.

161. 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.

162. 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 Data Breach.

163. Because of the Data Breach, 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.

164. As a result of the Data Breach, 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 Data Breach. Specifically, Plaintiff Telford has devoted time to, among other things, investigating the Data Breach, 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 Data Breach, Plaintiff Telford also lost personal funds to pay for gas to the nearest U-Haul location.

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

166. Plaintiff Telford has suffered injury directly and proximately caused by the Data Breach, 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; and (e) 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.

V.CLASS ALLEGATIONS

167. Plaintiffs bring this nationwide 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.

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

> All individuals whose PII was compromised in the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "Nationwide Class" or "Class").

169. The Arizona Subclass that Plaintiff Frierson seeks to represent is defined as follows:

> All individuals who resided in Arizona at any time during, and whose PII was compromised in, the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "Arizona Subclass").

170. The New York Subclass that Plaintiff Dobson seeks to represent is defined as follows:

> All individuals who resided in New York at any time during, and whose PII was compromised in, the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "New York Subclass").

171. The California Subclass that Plaintiffs Hendricks, Anderson, and Telford seek to represent is defined as follows:

> All individuals who resided in California at any time during, and whose PII was compromised in, the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "California Subclass").

172. The Pennsylvania Subclass that Plaintiff Proctor seeks to represent is defined as follows:

> All individuals who resided in Pennsylvania at any time during, and whose PII was compromised in, the data breach that is the subject

> of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "Pennsylvania Subclass").

173. The Oregon Subclass that Plaintiff Gibson seeks to represent is defined as follows:

> All individuals who resided in Oregon at any time during, and whose PII was compromised in, the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "Oregon Subclass").

174. The Indiana Subclass that Plaintiff Lauderdale seeks to represent is defined as follows:

> All individuals who resided in Indiana at any time during, and whose PII was compromised in, the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "Indiana Subclass").

175. The Virginia Subclass that Plaintiff Durgan seeks to represent is defined as follows:

> All individuals who resided in Virginia at any time during, and whose PII was compromised in, the data breach that is the subject of the *Notice of Recent Security Incident* that Defendant sent to Plaintiffs and Class Members on or around September 9, 2022 (the "Virginia Subclass").

176. 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.

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

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

179. 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 Breach;

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 Breach;

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

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

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

m. 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 Breach.

180. 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 Breach, due to Defendant's misfeasance.

181. 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.

182. 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.

183. 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.

184. 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.

185. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

187. 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 Breach, and Defendant may continue to act unlawfully as set forth in this complaint.

188. 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.

189. 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 an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

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

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. 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
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

190. Plaintiffs re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

191. Plaintiffs bring this Count on behalf of themselves and on behalf of the Nationwide Class.

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

193. Plaintiffs and the Nationwide Class provided and entrusted their PII to Defendant under the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

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

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

196. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

197. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

198. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

199. Defendant also had a duty to protect against the reasonably foreseeable criminal conduct of a third party as it was on notice that the failure to protect the PII that it collected for its own pecuniary benefit would result in harm to Plaintiffs and the Nationwide Class.

200. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

201. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

202. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's

inadequate security practices.

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

204. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

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

206. Defendant was in an exclusive position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

207. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

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

209. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise

reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

210. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

211. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

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

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

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

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

216. There is a close causal connection between Defendant's failure to implement

security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

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

218. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm,

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

219. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

220. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

221. Plaintiffs re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

222. Plaintiffs bring this Count on behalf of themselves and on behalf of the Nationwide Class.

223. When Plaintiffs and Class Members provided their PII to Defendant in exchange for rental and storage services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

224. Defendant required Plaintiffs and Class Members to provide their PII in order for them to use Defendant's services. Plaintiffs and the Nationwide Class did so provide and

entrusted their PII to Defendant. In so doing, Plaintiffs and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their PII had been compromised or stolen.

225. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of the Data Breach.

226. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

227. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

228. Defendant's parent company's 2021 Annual Report, filed with the SEC in July 2021, represents that "Our information systems are largely Internet-based, including our point-of-sale reservation system, payment processing and telephone systems. While our reliance on this technology lowers our cost of providing service and expands our abilities to better serve customers, it exposes us to various risks including natural and 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."[24]

[24] AMERCO 2021 Annual Report, *available at* https://www.amerco.com/reports.aspx (last visited Dec. 13, 2022). AMERCO is Defendant's parent company.

229. Defendant's conduct and statements confirm that Defendant intended to bind itself to protect the PII that Plaintiffs and the Nationwide Class entrusted to Defendant.

230. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

231. Defendant breached the implied contracts it made with Plaintiffs and the Nationwide Class by (i) failing to use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of Plaintiffs' and the Nationwide Class's PII, (ii) failing to encrypt driver's license numbers and other sensitive PII, (iii) failing to delete PII it no longer had a reasonable need to maintain, and (iv) otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

232. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their sensitive information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

233. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Violations of the Drivers Privacy Protection Act, 18 U.S.C. § 2721, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

234. Plaintiffs re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

235. Plaintiffs bring this Count on behalf of themselves and on behalf of the Nationwide Class.

236. Defendant knowingly obtained Plaintiffs' and the Nationwide Class's Personal Information, from a motor vehicle record, including their driver's licenses.

237. Defendant voluntarily decided to populate its customer contracts when accessed via its contract search tool with Plaintiffs' and the Nationwide Class's Personal Information, including their driver's license numbers.

238. Defendant reasonably should have known that populating its customer contracts when accessed via its contract search tool would disclose Plaintiffs' and the Nationwide Class's driver's license numbers to cybercriminals for impermissible purposes.

239. In failing to implement reasonable measures to prevent the Data Breach, Defendant disclosed Plaintiffs' and the Nationwide Class's driver's license numbers for an impermissible purpose.

240. Each of Plaintiffs and Class Members demand actual damages, but not less than liquidated damages in the amount of $2,500, punitive damages upon proof of willful or reckless disregard of the law, reasonable attorney's fees and other litigation costs reasonably incurred, and such other preliminary and equitable relief as the court determines to be appropriate.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

241. Plaintiffs re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

242. Plaintiffs bring this Count on behalf of themselves and on behalf of the Nationwide Class.

243. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

244. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs and the Nationwide Class allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs and the Nationwide Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will

occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

245. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Nationwide Class's PII, including driver's license numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the driver's license number of Plaintiffs and the Nationwide Class.

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

a. Defendant owes a legal duty to secure the PII of past and current customers of Defendant;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and the Nationwide Class harm.

247. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

248. If an injunction is not issued, Plaintiffs and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

249. The hardship to Plaintiffs and the Nationwide Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Nationwide Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

250. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the Nationwide Class and others whose confidential information would be further compromised.

COUNT V
Violations of the Arizona Consumer Fraud Act,
A.R.S. §§ 44-1521, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively,
Plaintiff Frierson and the Arizona Subclass)

251. Plaintiffs and the Class or, alternatively, Plaintiff Frierson and the Arizona Subclass, re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

252. U-Haul is a "person" as defined by A.R.S. §44-1521(6).

253. U-Haul sold Plaintiffs and Class Members "merchandise" as defined by A.R.S. § 44-1521, in the form of services, including vehicle and storage rental services.

254. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

A.R.S. § 44-1522(A).

255. U-Haul used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

256. U-Haul omitted and concealed material facts, which it knew about and had the duty to disclose—namely, U-Haul's inadequate privacy and security protections for Plaintiffs' and Class Members' Private Information. This omission was designed to mislead consumers.

257. U-Haul omitted and concealed those material facts, even though in equity and good conscience those facts should have been disclosed, and did so with the intent that others would rely on the omission, suppression, and concealment.

258. Upon information and belief, U-Haul intentionally omitted and concealed material facts—like U-Haul's inadequate cyber and data privacy and security protections—with the intention that consumers rely on those omissions.

259. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

260. Plaintiffs and Class Members were ignorant of the truth and relied on the concealed facts in providing Private Information to U-Haul and incurred damages as a consequent and proximate result.

261. But for U-Haul's omissions, the damage to Plaintiffs and Class Members would not have occurred.

262. Plaintiffs do not allege any claims based on any affirmative misrepresentations by U-Haul. Rather, Plaintiffs allege that U-Haul omitted, failed to disclose, and concealed material facts and information as alleged herein—despite its duty to disclose such facts and information.

263. U-Haul knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, and that the risk of a data breach or theft was highly likely. U-Haul's actions in engaging in these deceptive acts and practices were intentional, knowing and willful, and wanton and reckless with respect to the rights of Plaintiffs and Class Members.

264. Specifically, U-Haul failed to comply with the standards outlined by the FTC regarding protecting PII. U-Haul was or should have been aware of these standards. U-Haul's

data security systems did not follow the FTC's guidelines. And thus, U-Haul's systems operated below the minimum standards.

265. Plaintiffs and Class Members were ignorant of the truth and relied on the concealed facts in providing their Private Information and incurred damages as a consequent and proximate result.

266. Plaintiffs and Class Members seek all available relief under A.R.S. § 44-1521, *et seq*., including, but not limited to, compensatory damages, statutory punitive damages, injunctive relief, and attorneys' fees and costs.

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

267. Plaintiffs Hendricks, Anderson, and Telford re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

268. Plaintiffs Hendricks, Anderson, and Telford ("Plaintiffs" for the purposes of this Count) brings this Count on their own behalf and on behalf of the California Subclass.

269. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting 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."[25]

[25] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

270. 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 Breach.

271. 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).

272. 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.

273. Plaintiffs and California Subclass 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."

274. 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.

275. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and California Subclass members' unencrypted first and last names and Social Security numbers among other information.

276. Plaintiffs' and California Subclass 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.

277. The Data Breach 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 California Subclass members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiffs' and California Subclass members' PII as a result of this attack.

278. More than 30 days from the filing of this Complaint, Plaintiffs Hendricks, Anderson, and Telford, respectively, provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant failed to respond and has not cured or is unable to cure the violations described therein. 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 up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

279. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII
Violations of California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On behalf of Plaintiffs Hendricks, Anderson, Telford and the California Subclass)

280. Plaintiffs Hendricks, Anderson, and Telford re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

281. Plaintiffs Hendricks, Anderson, and Telford ("Plaintiffs" for the purposes of this Count) bring this Count on their own behalf and on behalf of the California Subclass.

282. The UCL prohibits any "unlawful" or "unfair" business act or practice, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

283. In the course of conducting its business, Defendant committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and California Subclass members' Private Information, and by violating the statutory and common law alleged herein, including, inter alia, the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, et seq.), Article I, Section 1 of the California Constitution (California's constitutional right to privacy), Cal. Civil Code § 1798.81.5, 45 C.F.R. § 164, et seq., and Section 5 of the FTC Act. Plaintiffs and California Subclass members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

284. Defendant also violated the UCL by failing to timely notify Plaintiffs and California Subclass members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their Private Information. If Plaintiffs and California Subclass

members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their Private Information and identities.

285. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Subclass members' Private Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass members. They were likely to deceive the public into believing their Private Information was securely stored when it was not. The harm these practices caused to Plaintiffs and California Subclass members outweighed their utility, if any.

286. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect Private Information and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

287. Plaintiffs and California Subclass members suffered injury in fact and lost money or property as a result of Defendant's violations of statutory and common law. Plaintiffs and the California Subclass suffered from overpaying for services that should have included adequate data security for their Private Information, by experiencing a diminution of value in their Private Information as a result if its theft by cybercriminals, the loss of Plaintiffs' and California Subclass members' legally protected interest in the confidentiality and privacy of their Private Information, and additional losses as described above.

288. Plaintiffs and California Subclass members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

289. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. As such, Plaintiffs, on behalf of themselves and California Subclass members, seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the

Private Information entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203. To the extent any of these remedies are equitable, Plaintiffs and the Class seek them in the alternative to any adequate remedy at law they may have.

COUNT VIII
Violations of the New York General Business Law,
NY G.B.L. § 349
(On Behalf of Plaintiff Dobson and the New York Subclass)

290. Plaintiff Dobson and the New York Subclass, re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

291. Defendant violated New York's General Business Law § 349(a) when it engaged in deceptive, unfair, and unlawful trade, acts, or practices in conducting trade or commerce and through furnishing of services, including but not limited to:

a. Misrepresenting material facts to Plaintiff Dobson and the New York Subclass by stating it would maintain adequate security measures to protect from unauthorized disclosure the PII belonging to Plaintiff Dobson and the New York Subclass;

b. Misrepresenting material facts to Plaintiff Dobson and the New York Subclass by representing itself as a business that would comply with state and federal laws pertaining to the privacy and security of PII belonging to Plaintiff Dobson and the New York Subclass;

c. Omitting and/or concealed material facts regarding its inadequate privacy and security protections for PII belonging to Plaintiff Dobson and the New York Subclass;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain sufficient privacy and security related to PII belonging to Plaintiff Dobson and the New York Subclass resulting in a data breach, which is in violation of duties imposed on Defendant by state and federal laws, including the Federal Trade Commission Act (15 U.S.C. § 45);

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff Dobson and the New York Subclass in a timely and accurate manner, which violates duties imposed on Defendant by New York General Business Law § 899-aa(2).

292. Defendant knew, or should have known, that its computer systems and security practices were inadequate to protect PII entrusted to Defendant by Plaintiff Dobson and the New York Subclass. Further, Defendant knew, or should have known, that the risk of theft of PII through a data breach was highly probable.

293. Defendant was in a superior position to know the true facts regarding its deficient data security and should have disclosed this fact to the Plaintiff Dobson and New York Subclass.

294. Defendant mislead consumers regarding the security of its network and ability to secure PII it collected by failing to disclose the true facts regarding its deficient data security. This constitutes false and misleading representation, which had the capability, tendency, and

impact of deceiving or misleading consumers, such as Plaintiff Dobson and the New York Subclass.

295. Defendant's representations were material representations, which consumers such as Plaintiff Dobson and the New York Subclass relied upon to their detriment.

296. The representations as well as Defendant's conduct towards Plaintiff Dobson and the New York Subclass occurred in New York where Plaintiff Dobson and the New York Subclass engaged the services of and entrusted their PII to Defendant.

297. Defendant's conduct is unconscionable, deceptive, and unfair, and is substantially likely to and did mislead consumers such as Plaintiff Dobson and the New York Subclass acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff Dobson and the New York Subclass have been injured because they were not timely notified of the Data Breach causing their PII to be compromised.

298. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff Dobson and the New York Subclass had their PII disclosed to unauthorized third parties, which caused damage to Plaintiff Dobson and the New York Subclass.

299. Plaintiff Dobson and the New York Subclass seek relief under New York General Business Law § 349(h), including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and/or attorney's fees, expenses, and costs.

COUNT IX
Violation of Oregon's Unlawful Trade Practices Act ("UTPA")
ORS § 646.608 et seq.
(On Behalf of Plaintiff Gibson and the Oregon Subclass)

300. Plaintiff Gibson ("Plaintiff" for the purposes of this Count) and the Oregon Subclass (the "Class" for the purposes of this Count), re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

301. The Data Breach constituted a "breach of security" of U-Haul, within the meaning of O.R.S. § 646.602(1)(a).

302. The information lost in the Data Breach constituted "personal information" within the meaning of ORS § 646.602(11).

303. U-Haul failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

304. U-Haul unreasonably delayed informing anyone about the breach of security of Class Members' confidential and personal information after U-Haul knew the Data Breach had occurred.

305. U-Haul failed to disclose to Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal Information when they knew or reasonably believed such information had been compromised.

306. Upon information and belief, no law enforcement agency instructed U-Haul that notification to Class Members would impede any investigation.

307. U-Haul's failure to implement reasonable security measures, promptly notify Class Members, and otherwise comply with ORS § 646A.600 is an unlawful practice under ORS § 646.607(1)(u) in that U-Haul engaged in unfair and deceptive conduct.

308. U-Haul knew or should have known that its data security practices were inadequate to protect against the known and foreseeable risk of a data breach. Plaintiff and Class Members relied on U-Haul to promptly and accurately disclose the true state of its data security practices, U-Haul omitted such information from disclosure to Plaintiff and Class Members, and Plaintiff and Class Members considered the omitted information material to their decision to transact with Defendant. Plaintiff and Class Members would not have purchased the goods or services from U-Hauls or would have paid less had they known about Defendant's deficient data security.

309. As a result of Defendant's failures and omissions Plaintiff and Class Members suffered damages, including in the form of loss of the benefit-of-the bargain, time and/or money spent mitigating harms, diminished value of PII, and/or attempted identity theft or misuse of PII.

310. U-Haul's failure to safeguard Plaintiff's and Class Members' private and financial data constitutes an unfair act because these acts or practices offend public policy as it has been established by statutes, regulations, the common law or otherwise, including, but not limited to, the public policy established by ORS § 646A.600.

311. U-Haul's failure to safeguard Plaintiff's and Class Members' private and financial data is unfair because this act or practice (1) causes substantial injury to Plaintiff and

Class Members; (2) is not outweighed by any countervailing benefits to consumers or competitors; and (3) is not reasonably avoidable by consumers.

312. U-Haul's failure to safeguard Plaintiff's and Class Members' private and financial data is unfair because this act or practice is immoral, unethical, oppressive and/or unscrupulous.

313. U-Haul's failure to promptly notify Plaintiff and Class Members of the loss of their data is unfair because these acts or practices offend public policy as it has been established by statutes, regulations, the common law or otherwise, including, but not limited to, the public policy established by ORS § 646A.600.

314. U-Haul's failure to promptly notify Plaintiff and Class Members of the loss of their data is unfair because this act or practice (1) causes substantial injury to Plaintiff and Class Members; (2) is not outweighed by any countervailing benefits to consumers or competitors; and (3) is not reasonably avoidable by consumers.

315. U-Haul's failure to promptly notify Plaintiff and Class Members of the loss of their data is unfair because this act or practice is immoral, unethical, oppressive and/or unscrupulous.

316. As a result of U-Haul's violation of ORS § 646.605 et seq., Plaintiff and other Class Members suffered ascertainable loss of money or property, including expenses associated with necessary credit monitoring.

317. Plaintiff, individually and on behalf of the Class, seeks all remedies available under ORS § 646.605, including equitable relief, actual damages, statutory damages pursuant to ORS § 646.638(1), and punitive damages.

318. Plaintiff, individually and on behalf of the Class, also seeks reasonable attorneys' fees and costs under ORS § 646.638(3).

COUNT X
Violations of the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-1, *et seq.* ("IDCSA")
(On Behalf of Plaintiff Lauderdale and the Indiana Subclass)

319. Plaintiff Lauderdale ("Plaintiff," for purposes of this Count) and the Indiana Subclass re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

320. Ind. Code § 24-5-0.5-3(a) prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

321. Defendant is a "supplier" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions," in violation of the IDCSA. As a regular part of its business, Defendant provides vehicle and storage unit rentals and related products to individuals residing in Indiana. Defendant accepts payments from customers, like Plaintiff, online, in person or by mail. Transactions were directed towards Indiana, and on information and belief, those transactions were processed in Indiana.

322. In connection with their consumer transactions, Defendant engaged in unfair, abusive or deceptive acts, omissions or practices by, inter alia, engaging in the following conduct:

a. failing to maintain sufficient security to keep sensitive PII of Plaintiff and the Indiana Subclass members from being hacked and stolen;

b. misrepresenting and omitting material facts to Plaintiff and the Indiana Subclass members in connection with the sale of goods or services, by

representing that it would maintain adequate data privacy and security practices and procedures to safeguard their PII from unauthorized disclosure, release, data breaches, and theft, including but not limited to promises made in its privacy policies;

c. misrepresenting and omitting material facts to Plaintiff and the Indiana Subclass members, in connection with the sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of their PII, such requirements included, but are not limited to, those imposed by laws such as the Federal Trade Commission Act (15 U.S.C. § 45) and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and

d. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Indiana Subclass members' PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

323. Defendant knew that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and the Indiana Subclass members, and that risk of a data breach or theft was highly likely. Nevertheless, Defendant did nothing to warn them about its data insecurities, and instead affirmatively promised that it would maintain adequate security. This was a deliberate effort to mislead customers, such as Plaintiff and the Indiana Subclass members, to encourage them to use Defendant's services.

324. The above unfair and deceptive practices and acts by Defendant were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

325. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and the Indiana Subclass members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their financial and personal information and damages.

326. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and the Indiana Subclass members are now likely to suffer identity theft crimes, and they face a lifetime risk of identity theft crimes.

327. The IDCSA provides that "[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater." § 24-5-0.5-4(a). Moreover, "[t]he court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (1) three (3) times the actual damages of the consumer suffering the loss; or (2) one thousand dollars ($1,000)." *Id*.

328. The IDCSA provides that a senior consumer, defined as "an individual who is at least sixty (60) years of age," may recover treble damages for an incurable deceptive act. *Id*. §§ 24-5-0.5-2(a)(9), 24-5-0.5-4(i).

329. Plaintiff and the Indiana Subclass members seek relief under Ind. Code § 24-5-0.5-4, including, but not limited to, the maximum statutory damages available under the IDCSA, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

COUNT XI
Violations of Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"),
73 Pa. Stat. Ann. § 201-1, *et seq.*
(On Behalf of Plaintiff Proctor and the Pennsylvania Subclass)

330. Plaintiff Proctor ("Plaintiff" for the purposes of this Count) and the Pennsylvania Subclass (the "Class" for the purposes of this Count), re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

331. Defendant violated Pennsylvania's UTPCPL when it engaged in deceptive, unfair, and unlawful trade, acts, or practices in conducting trade or commerce and through furnishing of services, including but not limited to:

a. Misrepresenting and omitting material facts to Plaintiff and the Class by stating it would maintain adequate security measures to protect from unauthorized disclosure the PII belonging to Plaintiff and the Class;

b. Misrepresenting and omitting material facts to Plaintiff and the Class by representing itself as a business that would comply with state and federal laws pertaining to the privacy and security of PII belonging to Plaintiff and the Class;

c. Omitting and/or concealing material facts regarding its inadequate privacy and security protections for PII belonging to Plaintiff and the Class;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain sufficient privacy and security related to PII belonging to Plaintiff and the Class resulting in a data breach, which is in violation of duties imposed on Defendant by state and federal laws, including the Federal Trade Commission Act (15 U.S.C. § 45);

e. Engaging in deceptive, unfair, and unlawful trade acts or practices relating to its Privacy Policy, which violates duties imposed on Defendant by 18 Pa.C.S.A. § 4107(10).

332. Defendant knew, or should have known, that its computer systems and security practices were inadequate to protect PII entrusted to Defendant by Plaintiff and the Class. Further, Defendant knew, or should have known, that the risk of theft of PII through a data breach was highly probable.

333. Defendant was in a superior position to know the true facts regarding its deficient data security and should have disclosed this fact to Plaintiff and the Class.

334. Defendant misled consumers regarding the security of its network and ability to secure PII it collected by failing to disclose the true facts regarding its deficient data security. This constitutes a false and misleading representation, which had the capability, tendency, and impact of deceiving or misleading consumers, such as Plaintiff and the Class.

335. Defendant's representations and omissions were material to consumers such as Plaintiff and the Class who reasonably relied on Defendant to disclose the true condition of its data security practices.

336. Defendant's conduct is unconscionable, deceptive, and unfair, and is substantially likely to and did mislead consumers such as Plaintiff and the Class acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have been injured because they were not timely notified of the Data Breach causing their PII to be compromised.

337. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff and the Class had their PII disclosed to unauthorized third parties, which caused damage to Plaintiff and the Class.

338. Plaintiff, individually and on behalf of the Class, seeks all remedies available under the UTPCPL, including equitable relief, actual damages, statutory damages pursuant to 73 Pa. Stat. Ann. § 201-9.2, and punitive damages. Plaintiff, individually and on behalf of the Class, also seeks reasonable attorneys' fees and costs.

COUNT XII
Violation of the Virginia Consumer Protection Act
Va. Code. Ann. §§ 59.1-196, *et seq.*
(On Behalf of Plaintiff Durgan and the Virginia Subclass)

339. Plaintiff Durgan ("Plaintiff" for the purposes of this Count) and the Virginia Subclass (the "Class" for the purposes of this Count), re-allege and incorporate by reference paragraphs 1-220 as if fully set forth herein.

340. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

341. Defendant is a "person" as defined by Va. Code Ann. § 59.1-198.

342. Defendant is a "supplier," as defined by Va. Code Ann. § 59.1-198.

343. Defendant engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Defendant advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

344. Defendant engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures, by and through making the representations included in the Privacy Policy, among others;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, by and through making the representations included in the Privacy Policy among others;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

345. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

346. Defendant's representations and omissions, made at the time of the relevant transactions, were material because they were likely to deceive reasonable consumers, including Plaintiff and Class members, about the adequacy of Defendant's computer and data security and the quality of the Defendant's brands.

347. Had Defendant disclosed to Plaintiff and Class Members that their data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class Members' PII as part of the services Defendant provided and for which Plaintiff and Class Members paid without advising Plaintiff and Class Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' PII. Accordingly, Plaintiff and the Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered. And, had they been forewarned, Plaintiff and Class Members would have sought

alternative service providers.

348. Defendant had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Class—and Defendant, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Class that contradicted these representations.

349. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

350. Defendant acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Class Members' rights. Defendant's past data breaches and breaches within the hospital industry put them on notice that their security and privacy protections were inadequate. An award of punitive damages would serve to punish Defendant for its wrongdoing, and warn or deter others from engaging in similar conduct.

351. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

352. Defendant's violations present a continuing risk to Plaintiff and Class Members as well as to the general public.

353. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

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 Nationwide Class and state subclasses and appointing Plaintiffs and their Counsel to represent such Classes;

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 Plaintiff, 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: January 4, 2023.

Respectfully Submitted,

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

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

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

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

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

William B. Federman**
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
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
abm@murphylegalfirm.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
aberry@justice4you.com
gharoutunian@justice4you.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
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
Tel: (602) 892-0341
Fax: (855) 203-2035
jennifer.rethemeier@drlawllp.com
paul@drlawllp.com

Marc E. Dann*
Brian D. Flick*
DANNLAW
15000 Madison Avenue

Lakewood, OH 44107
mdann@dannlaw.com
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
Sharon A. Harris**
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
tom@attorneyzim.com
sharon@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
rdm@tblaw.com
cjw@tblaw.com
apb@tblaw.com
cml@tblaw.com

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

Attorneys for Plaintiffs and the Proposed Nationwide Class and Subclasses
**pro hac vice*
***pro hac vice* anticipated

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 4th day of January, 2023, 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)