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

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

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-247-0047
gklinger@milberg.com

Counsel for Plaintiff and the Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Joseph Laventure, Jr., individually and on behalf of all others similarly situated, Plaintiff, v. U-Haul International, Inc., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY DEMAND**

Plaintiff Joseph Laventure, Jr. ("Plaintiff") brings this Class Action Complaint against U-Haul International, Inc. ("Defendant" or "U-Haul"), in his individual capacity and on behalf

of all others similarly situated, and alleges, upon personal knowledge as to his own actions, his counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving U-Haul International Inc., an international for-profit rental vehicle and storage company.[1]

2. U-Haul International failed to reasonably secure, monitor, and maintain the Personally Identifiable Information ("PII") provided by its consumers, including, without limitation, names, dates of birth, and driver's license numbers or state identification cards (Collectively, "PII" or "PII"). Upon information and belief, the Data Breach resulted in the likely unauthorized access, download, exfiltration, and misuse of the PII by the cyber criminals who targeted that information for nefarious purposes.

3. The full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of the litigation.

4. The Privacy Policy posted by Defendant on its website states "[w]e use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your Information and our systems.."[2] On information and belief, Defendant failed to honor this promise.

5. Upon information and belief, Defendant obtained the PII of Plaintiff and Class Members as customers and stored that PII, unencrypted, in an Internet-accessible environment

[1] *See* https://www.uhaul.com/About/History/ (last visited Sept. 19, 2022).
[2] *See* https://www.uhaul.com/Legal/PrivacyPolicy/#Security (last visited Sept. 19, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

on Defendant's network.

6. On or before August 1, 2022, Defendant learned of a data security incident on its network which took place between November 5, 2021, and April 5, 2022.

7. Eventually, Defendant determined that an unknown actor compromised two unique passwords for accessing Defendant's search tool and database and was thereby able to access the contracts of Plaintiff and Class Members as current or former customers of Defendant.

8. On or around September 9, 2022, Defendant began notifying Class Members of the Data Breach.

9. When Defendant began obtaining, collecting, using, and otherwise deriving benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to protect and safeguard that PII from unauthorized access and intrusion.

10. Hackers often access and sell PII on the dark web to criminals, which exposes people like Plaintiff and Class Members to a lifetime risk of identity theft and other detrimental uses of their PII. This risk is heightened for Plaintiff and Class Members because the PII compromised contained their driver's license numbers and/or state identification numbers.

11. Plaintiff's and Class Members' PII was compromised due to Defendant's negligence and/or recklessness in failing to safeguard and protect the PII it collected from its customers. Not only did Defendant fail to prevent the Data Breach, but Defendant failed to discover the Data Breach in a reasonable amount of time and then delayed several months to report the Data Breach to the SEC and the affected individuals. Further, Defendant has failed to disclose the vulnerabilities that led to the Data Breach and how Defendant has addressed the

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

root causes.

12. Because of Defendant's failure to discover the Data Breach in a reasonable period of time, and because of Defendant's failure to quickly disclose the breach to Plaintiff and Class Members, Plaintiff and Class Members were unaware that their PII was compromised for months. They were unaware that they were, and still are, at a heightened risk of identity theft and fraud due the Defendant's acts and omissions.

13. Plaintiff brings this action on behalf of all persons whose PII was compromised in the Data Breach as a result of Defendant's failure to properly protect and safeguard the PII of Plaintiff and Class Members, failure to timely disclose the Data Breach and warn Plaintiff and Class Members of the danger, and failure to employ reasonable and standard security procedures to prevent vulnerabilities and security incidents like this.

14. Plaintiff and Class Members suffered injury as a result of Defendant's conduct, including: (1) the loss or diminution in value of PII; (2) out-of-pocket expenses to prevent, detect, and recover from the unauthorized misuse of their PII; (3) loss of time and lost opportunity costs associated with attempts to mitigate the consequences of the Data Breach; (4) the unauthorized disclosure of their PII; and (5) the increased and continued risk of misuse of their PII (which remains in the hands of unauthorized third parties and, upon information and belief, remains unprotected and unencrypted in the possession of Defendant).

15. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

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

17. Accordingly, Plaintiff, on behalf of himself and other Class Members, asserts claims for Negligence (Count I), Breach of Implied Contract (Count II), Unjust Enrichment (Count III), and Violation of The Drivers Privacy Protection Act, 18 U.S.C. Section 2721, *et seq*. (Count IV).

I. THE PARTIES

Plaintiff Joseph Laventure, Jr.

18. Plaintiff Joseph Laventure, Jr. is, and at all times relevant has been, a resident and citizen of Manassas, Virginia. Plaintiff received a "Notice of Data Breach" email dated September 13, 2022, on or about that date. The letter notified Plaintiff that on August 1, 2022, U-Haul International, Inc., determined that some of its rental contracts had been improperly accessed. It further stated that U-Haul determined that "two unique passwords that were used to access a customer contract search tool that allows access to rental contracts for U-Haul customers." The type of data contained in these contracts and obtained by the unauthorized attacker included full names, addresses, telephone numbers, dates of birth, email addresses, and driver's license numbers. The letter further advised that Plaintiff and should monitor his credit with credit reports, and "remain vigilant."

19. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff. Plaintiff would not have entrusted his PII to Defendant had he

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

Defendant U-Haul International, Inc.

20. Defendant U-Haul International, Inc., is a Nevada corporation with its principal place of business located in Phoenix, Arizona. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

II. JURISDICTION AND VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d). 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.

22. This Court has general jurisdiction over the Defendant because U-Haul International, Inc., is a citizen of Arizona and Nevada because it is incorporated in Nevada and has its principal place of business in Arizona. Additionally, the server implicated in this Data Breach is likely based in this District.

23. Venue is proper in this Court because a substantial part of the events giving rise to this action occurred in Maricopa County.

III. FACTUAL ALLEGATIONS

Background

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

24. Defendant provides vehicle and storage rental services to individuals internationally.

25. Plaintiff and Class Members were customers of Defendant whose PII was included in rental contracts required by Defendant to use its services.

26. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

27. Defendant voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. U-Haul has a legal duty to keep consumer's PII safe and confidential.

28. The information held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

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

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

The Data Breach

31. Defendant "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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

customers." According to Defendant, it uncovered this attack on August 1, 2022, though the attack took place between November 5, 2021 and April 5, 2022. Defendant has not stated why it took so long to discover the security breach.

32. Defendant acknowledged that "the accessed personal information includes your name and one or more of the following: address, telephone number, date of birth, email address and driver's license number."

33. Defendant's investigation was inconclusive as to whether or not the accessed data has been or will be misused by the hackers.

34. In addition to sending notices to Plaintiff and Class Members, Defendant also filed a notice with the SEC.

35. Defendant admitted in the Notice of Recent Security Incident and the SEC filing that an unauthorized actor accessed sensitive information about Plaintiff and Class Members, including name, date of birth, and driver's license number or state identification number.

36. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

37. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

38. To prevent and detect cyberattacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

39. To prevent and detect cyber-attacks Defendant could and should have

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[3]

40. To prevent and detect cyber-attacks or ransomware attacks Defendant could and

[3] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 11, 2021).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection; and,
- Turn on attack surface reduction rules and [Antimalware Scan Interface]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

for Office [Visual Basic for Applications].[4]

41. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

42. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

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

43. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

44. As part of being a customer of Defendant, Plaintiff and Class Members, are required to give their sensitive and confidential PII to Defendant. Defendant retains this information.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[4] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

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

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

48. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII.[5]

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

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

Defendant Knew or Should Have Known of the Risk Because Cyber Attacks Commonly Target PII

51. Defendant knew and understood unprotected or exposed PII is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

Value of Personally Identifiable Information

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without

[5] *See* https://www.uhaul.com/Legal/PrivacyPolicy/#Security (last visited Sept. 19, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

authority."[6] 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."[7]

53. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

54. 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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[6] 17 C.F.R. § 248.201 (2013).
[7] *Id*.
[8] *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 visited Jan. 19, 2022).
[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan 19, 2022).
[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 19, 2022).

impossible, to change—driver's license number, name, and date of birth.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[11]

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

57. In some ways, driver's license numbers are even more attractive than Social Security Numbers to threat actors and more dangerous to the consumer when compromised. Unlike a Social Security Number, a driver's license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend that immediate notice, replacement, and identity theft protections are put in place for a minimum of three years. Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

58. Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

[11] 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 Nov. 11, 2021).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Apply for credit cards;

Apply for financial loans (especially student loans);

Open bank accounts;

Obtain or create fake driver's licenses;

Given to police for tickets;

Provided to accident victims;

Collect government unemployment benefits;

Create and sell underage fake IDs;

Replace/access account information on:

LinkedIn,

Facebook/Meta,

WhatsApp,

Instagram;

Obtain a mobile phone;

Dispute or prove a SIM swap;

Redirect U.S. mail;

Apply for unemployment benefits;

Undocumented individuals may use them as a method to gain access to the U.S., and claim a lost or stolen passport;

Create a fake license as a baseline to obtain a Commercial Driver's License;

File tax returns or gain access to filed tax returns; and

Engage in phishing and other social engineering scams.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

59. Unsecured sites that contain or transmit PI, such as a driver's license, require notice to consumers when the data is stolen because it can be used to perform identity theft and other types of fraud. A threat actor is usually motivated by financial or political gain before it exerts time, and skill to compromise and exfiltrate. Over time, identity thieves have systematized their criminal activities to gather important pieces of a synthetic identity from multiple breaches and sources. The theft of a driver's license number is no less valuable in that endeavor than the theft of a Social Security Number, as demonstrated by these two unique identifiers carrying the same price on the darknet, and by the fact that the identity thieves have demonstrated a systematic and businesslike process for collecting these stolen driver's license numbers in this Unauthorized Data Disclosure and others committed against insurers.

60. The frequency of cyberattacks has increased significantly in recent years.[12] In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[13]

61. Cybersecurity Ventures, a leading researcher on cybersecurity issues, expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[12] *See The Cost of Cybercrime,* Accenture Security (2019), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (last accessed August 16, 2022).

[13] *Top Cyberattacks of 2020 and How to Build Cyberresiliency*, ISAC (Updated Feb. 3, 2021), https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last accessed August 16, 2022) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).

transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.[14]

62. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[15]

63. As alleged above, stolen PI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

64. When malicious actors infiltrate companies and exfiltrate the PI that those companies store or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[16] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman*

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[14] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2020*, Cybercrime Magazine (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last accessed August 16, 2022).

[15] Cedric Nabe, *Impact of COVID-19 on Cybersecurity*, Deloitte, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last accessed August 16, 2022); Interpol, *Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception*, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last accessed August 16, 2022).

[16] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce (Feb. 2, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited August 16, 2022).

Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

65. Consumers' PI remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. 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.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Alternatively, criminals are able to purchase access to entire company data breaches for $900 to $4,500.[19] (Note: the prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices described above when they reach the "flea market sites.")

66. The information compromised in the Unauthorized Data Disclosure 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. And the information compromised in the Unauthorized Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, as well as benefits accounts in various state benefits offices, compounding the identity theft and cycle of black market sales detailed above. The driver's license numbers compromised in this Unauthorized Data Disclosure are also more

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

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

[18] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited August 16, 2022).

[19] *In the Dark*, VPNOverview, 2019, online website about dark web pricing (last accessed September 13, 2022).

valuable because driver's license numbers are long lasting, and difficult and problematic to change.

67. Recently, Forbes writer Lee Mathews reported on Geico's unauthorized data disclosure that included driver's license numbers:

68. Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200.[20]

69. National credit reporting company, Experian, blogger Gayle Sato also emphasized the value of driver's license information to thieves and cautioned:

> Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.[21]

70. In fact, according to CPO Magazine, which specializes in news, insights, and resources for data protection, privacy, and cyber security professionals,

71. To those unfamiliar with the world of fraud, driver's license numbers might seem

---

[20] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, Forbes (April 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited August 16, 2022).

[21] Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?* (Nov. 3, 2021), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited August 16, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: " . . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.[22]

72. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, including Geico, Farmers, USAA, Kemper, Metromile, and American Family all in 2021, indicating both that this particular form of PI is in high demand[23] and also that Defendants knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[24]

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[22] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine (April 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited August 16, 2022).

[23] *Id.*

[24] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (last visited

73. In fact, when Geico announced that its online quoting platform was subject to a breach, its data breach notice filed with the California Attorney General explicitly stated that GEICO had "reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name."[25]

74. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application: "Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name."[26]

75. For example, the New York State Department of Financial Services issued an

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

August 16, 2022) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited August 16, 2022) (describing a scam involving drivers' license numbers and Progressive Insurance).

[25] *See GEICO Notice of Data Breach,* *https://www.documentcloud.org/documents/20618953-geico-data-breach-notice* (last visited Aug. 16, 2022), (notice filed with Calif. Attorney General dated April 9, 2021).

[26] Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TechCrunch (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name (last visited August 16, 2022).

industry letter on February 16, 2021, stating that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [NPI, including] websites that provide an instant quote. . . . [I]t received reports from two auto insurers in late December 2020 and early January 2021, that cybercriminals were targeting their websites that offer instant [] quotes [] to steal unredacted driver's license numbers. . . . . DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits...DFS [] has also discovered communications on cybercrime forums offering to sell techniques to access driver's license numbers from auto insurance websites and step-by-step instructions on how to steal them."[27]

76. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details, or to fraudulently manufacture new accounts for access and sale. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

77. Victims of drivers' license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

78. For example, the United States Government Accountability Office noted in a June

[27] Industry Letter, *supra*, note 1.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

2007 report on data breaches (the "GAO Report") that criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[28] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[29]

79. What is more, the fraudulent activity resulting from the Data Breach may not come to light for years.

80. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen 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.[30]

81. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including driver's license

---

[28] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown,* Government Accountability Office (June 2007), http://www.gao.gov/assets/270/262899.pdf (last visited August 16, 2021).

[29] *Id.*

[30] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 19, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

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

82. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

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

84. In the breach notification letter, Defendant made an offer of one year of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

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

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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Plaintiff Joseph Laventure, Jr.'s Experience

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

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

89. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members' PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues when the service number for enrollment does not work properly.

90. Plaintiff and Class Members have been further damages by the compromise of their PII.

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

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

93. Plaintiff Laventure stores any documents containing his PII in a safe and secure

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

location. And he diligently chooses unique usernames and passwords for his online accounts.

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

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

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

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

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

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

100. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

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

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

CLASS ALLEGATIONS

102. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> **All persons U-Haul International, N.A. identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

103. Excluded from the Classes 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; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

104. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time. The identities of Class Members are ascertainable through U-Haul International's records, Class Members' records, publication notice, self-identification, and other means.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

105. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether U-Haul unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether 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;

c. Whether U-Haul's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether U-Haul's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether U-Haul owed a duty to Class Members to safeguard their PII;

f. Whether U-Haul breached its duty to Class Members to safeguard their PII;

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

h. Whether U-Haul knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of U-Haul's misconduct;

j. Whether U-Haul's conduct was negligent;

k. Whether U-Haul's conduct was per se negligent; and,

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

punitive damages, and/or injunctive relief.

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

108. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

109. **Predominance.** U-Haul International has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

110. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for U-Haul International. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

111. U-Haul International has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

112. Likewise, particular issues under Federal 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 U-Haul International owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether U-Haul International's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether U-Haul International's failure to institute adequate protective security measures amounted to negligence;

d. Whether U-Haul International failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

113. Finally, all members of the proposed Class are readily ascertainable. U-Haul International has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

by U-Haul International.

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

114. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 113.

115. U-Haul International knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and 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.

116. U-Haul International had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

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

118. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

119. U-Haul International had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

120. U-Haul had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to A.R.S. § 18-501 - 18-552.

121. U-Haul International, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within U-Haul International's possession.

122. U-Haul International, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

123. U-Haul International, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within U-Haul International's possession might have been compromised and precisely the type of information compromised.

124. U-Haul International's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

125. As a result of U-Haul International's ongoing failure to notify Plaintiff and Class Members regarding what type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

126. U-Haul International's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

127. As a result of U-Haul International's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

128. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

129. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, U-Haul International is guilty of oppression, fraud, or malice, in that U-Haul International acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

130. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling U-Haul International to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

131. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 130 above as if fully set forth herein.

132. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

133. Plaintiff and Class Members paid money to Defendant and disclosed their PII in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

134. In its written privacy policies, Defendant U-Haul International expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

135. Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

136. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

137. When Plaintiff and Class Members provided their PII to Defendant U-Haul International as a condition of their employment or employee beneficiary status, or as a condition precedent to receiving medical or pharmaceutical care, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

138. Defendant solicited, invited, and then required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

139. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

140. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

141. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

142. Defendant breached their implied contracts with Class Members by failing to safeguard and protect their PII.

143. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

145. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii)

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

146. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 145.

147. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

148. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

149. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

150. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

151. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

152. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

153. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

154. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

155. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
VIOLATIONS OF THE DRIVER'S PROVACY PROTECTION ACT, 18 U.S.C. § 2721, *et seq.*
(On Behalf of Plaintiff and the Class)

156. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 155.

157. Defendant knowingly obtained Plaintiff's and Class Members' PII, including their driver's license numbers.

158. Defendant decided to maintain Plaintiff's and Class Members' driver's license numbers and incorporate them into its contract search tool, which was compromised by cybercriminals in this Data Breach.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

159. Defendant failed to implement reasonable measures to prevent the Data Breach and safeguard the driver's license numbers of Plaintiff and Class Members, and thereby disclosed said driver's license numbers for impermissible purposes.

160. For the injury suffered as a direct result of the acts and omissions of Defendant, Plaintiff and Class Members demand actual damages, liquidated damages in the amount of $2,500 per driver's license number unlawfully disclosed, putative damages upon proof of reckless or willful disregard of the law, reasonable attorneys' fees, costs, and expenses, and other such equitable relief as the Court deems appropriate.

PRAYER FOR RELIEF

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

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;

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

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

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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

described herein;

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

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

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

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

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

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

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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

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

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

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

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

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

xiv. requiring Defendant to implement, maintain, regularly review, and revise as

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

D. For an award of damages, including actual, statutory, nominal, and consequential 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

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

RESPECTFULLY SUBMITTED this 22nd day of September, 2022.

PEREZ LAW GROUP, PLLC

/s/ Cristina Perez Hesano
Cristina Perez Hesano, Esq.
Attorney for Plaintiff

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

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-247-0047
gklinger@milberg.com

Counsel for Plaintiff and the Class

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301