

Marc E. Dann (*pro hac vice* anticipated)  
Brian D. Flick (*pro hac vice* anticipated)

**DannLaw**  
15000 Madison Avenue  
Lakewood, OH 44107  
Telephone: (216) 373-0539  
Emails: [mdann@dannlaw.com](mailto:mdann@dannlaw.com); [notices@dannlaw.com](mailto:notices@dannlaw.com)

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)  
Sharon A. Harris (*pro hac vice* anticipated)  
**Zimmerman Law Offices, P.C.**  
77 W. Washington Street, Suite 1220  
Chicago, Illinois 60602  
Telephone: (312) 440-0020  
Email: [firm@attorneyzim.com](mailto:firm@attorneyzim.com)

Robert D. Mitchell, Arizona Bar No. 011922  
Christopher J. Waznik, Arizona Bar No. 032812  
Anne P. Barber, Arizona Bar No. 035591  
CM Matthew Luk, Arizona Bar No. 037238

 **TIFFANY & BOSCO**  
P.A.  
Camelback Esplanade II, Seventh Floor  
2525 East Camelback Road  
Phoenix, Arizona 85016  
Telephone (602) 255-6000  
E-mails: [rdm@tblaw.com](mailto:rdm@tblaw.com); [cjw@tblaw.com](mailto:cjw@tblaw.com); [apb@tblaw.com](mailto:apb@tblaw.com);  
[cml@tblaw.com](mailto:cml@tblaw.com)

*Counsel for Plaintiff*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ARIZONA**

Sandra Brown, individually and on behalf of all  
others similarly situated,

Plaintiff,

vs.

U-Haul International, Inc.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

(DEMAND FOR JURY TRIAL)

1 Plaintiff SANDRA BROWN (“Plaintiff”), individually and on behalf of all others  
2 similarly situated (“Plaintiff”), through her attorneys, brings this action against Defendant  
3 U-HAUL INTERNATIONAL, INC (“Defendant” or “U-Haul”), and alleges upon  
4 personal knowledge as to her own actions and experiences, and upon investigation,  
5 information, and belief as to all other matters, as follows:  
6

7 **INTRODUCTION**

8 1. This consumer data breach lawsuit arises out of Defendant’s failure to  
9 implement and maintain adequate security and safeguards with respect to its collection  
10 and maintenance of highly sensitive and confidential personal information of its  
11 customers, including names, dates of birth, and driver’s license or state identification  
12 numbers (the “PII”). Defendant’s insufficient and unreasonable data security practices  
13 caused, facilitated, and exacerbated the data breach and its impact on Plaintiff and Class  
14 members.  
15

16  
17 2. U-Haul is an American moving truck, trailer, and self-storage rental  
18 company, based in Phoenix, Arizona, that has been in operation since 1945.<sup>1</sup> U-Haul has  
19 a network of locations across the United States.  
20

21 3. By Defendant’s own admission, from at least November 5, 2021 to April 5,  
22 2022, an unauthorized person obtained access to Defendant’s customer contract search  
23 tool and customer rental contracts (the “Data Breach”). Although Defendant identified  
24 the incident as early as August 1, 2022, Defendant did not warn those most at risk—  
25 Plaintiff and Class members, until September 9, 2022.  
26

27  
28 <sup>1</sup> See <https://www.uhaul.com/About/History/> (last visited Sept. 19, 2022).

1           4.       On or about September 9, 2022, Defendant notified the Security Exchange  
2 Commission of the Data Breach.

3           5.       The Data Breach exposed Plaintiff’s and Class members’ highly personally  
4 identifiable information (“PII”) to criminals, including, but not limited to, name, date of  
5 birth, and driver’s license number or state identification number.  
6

7           6.       The PII that Defendant compromised, exposed, and criminals stole in the  
8 Data Breach consists of some of the most sensitive and damaging information when in  
9 the hands of criminals, including but not limited to: names, dates of birth, and driver’s  
10 license or state identification numbers.  
11

12           7.       The PII stolen in the Data Breach can be used by criminals alone, and in  
13 conjunction with other pieces of information, to perpetrate crimes against Plaintiff and  
14 Class members that can result in significant liability and damage to their money,  
15 property, creditworthiness, reputation, and their ability to pay current loans, improve their  
16 credit, and/or obtain loans on favorable terms in the future.  
17

18           8.       Plaintiff and Class members entrusted Defendant with their sensitive PII.  
19 Defendant understands the importance of protecting such information. For example, on  
20 its website and in written documents provided to Plaintiff and Class members, Defendant  
21 states:  
22

23                   We value our customers and their privacy. We never sell your  
24 personal information. This Privacy Policy covers entities within the  
25 U-Haul System (“We”, “Us”, “Our”). For purposes of this Privacy  
26 Policy, the U-Haul System shall be defined as: U-Haul International,  
27 Inc. (“U-Haul”), and its parent, affiliated entities, related companies,  
28 subsidiaries, and agents who operate the U-Haul System, pursuant to  
which, among other things, Rental Equipment, self-storage rooms,  
and U-Boxes® are provided to the public, various services are

1 rendered and products are sold. . . . Your privacy is important to  
2 us, and we believe it is important to share with you how We handle  
3 your information, and how you can control the collection, correction  
4 and/or deletion of information. We will not use or share your  
5 information with anyone except as described in this Privacy Policy. .  
6 . . We use commercially reasonable physical, managerial, and  
7 technical safeguards to preserve the integrity and security of your  
8 Information and our systems. . . . In the event that personal  
9 information is compromised as a result of a breach of security, We  
10 will promptly notify those persons whose personal information has  
11 been compromised, in accordance with the notification procedures  
12 set forth in this Privacy Policy, or as otherwise required by  
13 applicable law.

14 *See* <https://www.uhaul.com/Legal/PrivacyPolicy/> (last visited Sept.  
15 19, 2022).

16 9. Defendant's representations concerning privacy practices and data security  
17 were false. Defendant does not state the date that it began investigating the incident, only  
18 that on August 1, 2022, its investigation determined that some rental contracts were  
19 accessed between November 5, 2021 and April 5, 2022. Criminals breached Defendant's  
20 inadequately defended systems, and accessed and acquired electronic files containing the  
21 PII of Plaintiff and Class members. The criminals gained unauthorized access by  
22 thwarting, circumventing, and defeating Defendant's unreasonably deficient data security  
23 measures and protocols. Defendants did not start notifying Plaintiff and other Class  
24 members of the Data Breach until on or around September 9, 2022.

25 10. Plaintiff, individually, and on behalf of all persons similarly situated, seeks  
26 to be made whole for the losses incurred by Plaintiff and other victims of the Data  
27 Breach, and the losses that will be incurred in the future. Plaintiff also seek injunctive  
28 relief in the form of compliant data security practices, full disclosure regarding the  
disposition of the information in Defendant's systems, and monitoring and audits of

1 Defendant's security practices going forward because Defendant continues to collect,  
2 maintain, and store Plaintiff's and Class members' PII.

3 **PARTIES, JURISDICTION, AND VENUE**

4 11. Plaintiff is a citizen of Ohio.

5  
6 12. Defendant is a Nevada corporation with its principal place of business in  
7 Phoenix, Arizona.

8 13. The Court has original jurisdiction under the Class Action Fairness Act  
9 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving 100 or more  
10 Class members and the amount in controversy exceeds \$5,000,000, exclusive of interest  
11 and costs. Many members of the Class, including Plaintiff, are citizens of different states  
12 from Defendant.  
13

14 14. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2),  
15 and 1391(c)(2), as a substantial part of the events giving rise to the claims emanated from  
16 activities within this District, and Defendant conducts substantial business in this District.  
17

18 **GENERAL ALLEGATIONS**

19 ***The Data Breach***

20  
21 15. In its September 9, 2022 notice to Plaintiff and Class members ("Data  
22 Breach Notice"), Defendant states that an unauthorized person obtained access to  
23 Defendant's file storage servers containing the PII of Plaintiff and Class members. A true  
24 and correct copy of the Data Breach Notice sent to Plaintiff is attached as **Exhibit 1**.  
25

26 16. Information pertaining to Plaintiff's and Class members' contracts with  
27 Defendant was acquired by an unauthorized person in the Data Breach.  
28

1           17. Defendant states that Plaintiff’s and Class members’ names, dates of birth,  
2 and driver’s license or state identification numbers (the “PII”), provided in connection  
3 with contracts with Defendant, were accessed by unauthorized persons in the Data  
4 Breach. *See* **Exhibit 1**; *see also* U-Haul’s SEC Form 8-K Report dated Sept. 9, 2022.  
5 Defendant omitted from its Data Breach Notice that Plaintiff’s and Class members’ birth  
6 dates were also taken by criminals in the Data Breach, but Defendant admitted that their  
7 birth dates were taken in its SEC Form 8-K Report.

9           18. Since discovering the Data Breach, Defendant states that it is augmenting  
10 its security measures to guard against such incidents, and implementing additional  
11 security safeguards and controls on the search tool. *See* **Exhibit 1**. These are actions that  
12 should have been employed in the first place and they would have prevented or limited  
13 the impact of the Data Breach.  
14

15           19. Defendant discovered the Data Breach on or before August 1, 2022 but did  
16 not publicly announced the Data Breach and notify those who were placed at risk of  
17 identity theft, until September 9, 2022. Defendant waited over a month to send Data  
18 Breach Notices to persons whose PII was accessed by criminals in the Data Breach.  
19

20           20. In the Data Breach Notice, Defendant provided information to Plaintiff and  
21 Class members about additional steps they can take to help protect themselves, including  
22 obtaining credit monitoring and identity theft protection services to help them detect  
23 possible misuse of PII. *See* **Exhibit 1**.  
24

25           21. As a result of the Data Breach, Plaintiff and Class members have been and  
26 must continue to be vigilant and review their credit reports for incidents of identity theft,  
27  
28

1 and educate themselves about security freezes, fraud alerts, and other steps to protect  
2 themselves against identity theft. Defendant's Data Breach Notice also advises Plaintiff  
3 and Class members to do all of this.

4 ***Industry Standards for Data Security***

5  
6 22. Defendant is aware of the importance of safeguarding Plaintiff's and Class  
7 members' PII, that by virtue of its business it places Plaintiff's and Class members' PII at  
8 risk of being targeted by hackers.

9  
10 23. Defendant is aware that the PII that it collects, organizes, and stores, can be  
11 used by criminals to engage in crimes such as identity fraud and theft using Plaintiff's  
12 and Class members' PII.

13  
14 24. Because of Defendant's failure to implement, maintain, and comply with  
15 necessary cybersecurity requirements, Defendant was unable to protect Plaintiff's and  
16 Class members' information and confidentiality, and protect against obvious and readily  
17 foreseeable threats to information security and confidentiality. As a proximate result of  
18 such failures, criminals gained unauthorized access to Defendant's customer contract  
19 search tool for a period of approximately five (5) months, and acquired Plaintiff's and  
20 Class members' PII in the Data Breach without being stopped.

21  
22 25. Only after the attack was completed did Defendant begin to undertake basic  
23 steps recognized in the industry to protect Plaintiff's and Class members' PII.

24  
25 26. Defendant was unable to prevent the Data Breach, and was unable to detect  
26 the unauthorized access to vast quantities of sensitive and protected files containing  
27 protected information of Plaintiff and Class members for five (5) months. Discovery on  
28

1 Defendant, law enforcement investigators, and private investigators, will reveal more  
2 specific facts about Defendant’s deficient and unreasonable security procedures.

3 27. Security standards commonly accepted among businesses that store  
4 personal information using the Internet include, without limitation:

- 5
- 6 a) Maintaining a secure firewall configuration;
  - 7 b) Monitoring for suspicious or irregular traffic to servers;
  - 8 c) Monitoring for suspicious credentials used to access servers;
  - 9 d) Monitoring for suspicious or irregular activity by known users;
  - 10 e) Monitoring for suspicious or unknown users;
  - 11 f) Monitoring for suspicious or irregular server requests;
  - 12 g) Monitoring for server requests for personal information;
  - 13 h) Monitoring for server requests from VPNs; and
  - 14 i) Monitoring for server requests from Tor exit nodes.
- 15

16

17 28. The U.S. Federal Trade Commission (“FTC”) publishes guides for  
18 businesses for cybersecurity<sup>2</sup> and protection of personal information<sup>3</sup> which includes  
19 basic security standards applicable to all types of businesses.

20

21 29. The FTC recommends that businesses:

- 22 a) Identify all connections to the computers where you store sensitive  
23 information;

24

---

25 <sup>2</sup> See F.T.C., *Start with Security: A Guide for Business*, (June 2015),  
26 <https://www.ftc.gov/business-guidance/resources/start-security-guide-business> (last visited Sept.  
20, 2022).

27 <sup>3</sup> See F.T.C., *Protecting Personal Information: A Guide for Business*, (Oct. 2016),  
28 [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)  
information.pdf (last visited Sept. 20, 2022).



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

1           30.    The FTC has brought enforcement actions against businesses for failing to  
2 adequately and reasonably protect customer information, treating the failure to employ  
3 reasonable and appropriate measures to protect against unauthorized access to  
4 confidential consumer data as an unfair act or practice prohibited by Section 5 of the  
5 Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these  
6 actions further clarify the measures businesses must take to meet their data security  
7 obligations.<sup>4</sup>

9           31.    Because Defendant was entrusted with consumers’ PII, it had and has a  
10 duty to keep the PII secure.

12           32.    Plaintiff and Class members reasonably expect that when they provide their  
13 PII to a company, the company will safeguard their PII.

14           33.    Despite Defendant’s obligations, Defendant failed to upgrade and maintain  
15 its data security systems in a meaningful way so as to prevent the Data Breach.

17           34.    Specifically, in breach of its duties, Defendant failed to:

- 18                   a)    Replace email filtering tools, malware software, and Internet  
19 monitoring tools with more robust solutions that utilize artificial  
20 intelligence (“AI”) to detect and block known and newly introduced  
21 malware;
- 22                   b)    Block all inbound and outbound Internet, email, and network traffic  
23 to foreign countries;
- 24                   c)    Maintain a secure firewall configuration;
- 25                   d)    Monitor for suspicious or irregular traffic to servers;

---

26  
27 <sup>4</sup> F.T.C., *Privacy and Security Enforcement: Press Releases*, [https://www.ftc.gov/news-](https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement)  
28 [events/media-resources/protecting-consumer-privacy/privacy-security-enforcement](https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement) (last visited  
Sept. 20, 2022).

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- e) Monitor for suspicious credentials used to access servers;
- f) Monitor for suspicious or irregular activity by known users;
- g) Monitor for suspicious or unknown users;
- h) Monitor for suspicious or irregular server requests;
- i) Monitor for server requests for personal information;
- j) Monitor for server requests from VPNs;
- k) Monitor for server requests from Tor exit nodes;
- l) Identify all connections to the computers where Defendant stores sensitive information;
- m) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- n) Scan computers on Defendant’s network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;
- o) Pay particular attention to the security of Defendant’s web applications—the software used to give information to visitors to its websites and to retrieve information from them;
- p) Use a firewall to protect Defendant’s computers from hacker attacks while they are connected to a network, especially the Internet;
- q) Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting its business;
- r) 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;

- 1 s) Monitor incoming traffic for signs that someone is trying to hack in.  
2 Keep an eye out for activity from new users, multiple log-in attempts  
3 from unknown users or computers, and higher-than-average traffic at  
4 unusual times of the day; and
- 5 t) Monitor outgoing traffic for signs of a data breach. Watch for  
6 unexpectedly large amounts of data being transmitted from their  
7 system to an unknown user. If large amounts of information are  
8 being transmitted from a business' network, the transmission should  
9 be investigated to make sure it is authorized.

10 35. Had Defendant properly maintained its systems and adequately protected  
11 them, it could have prevented the Data Breach.

12 ***Defendant Owed Duties to Plaintiff and Class Members***  
13 ***to Adequately Secure and Safeguard Their PII***

14 36. Defendant is aware of the importance of security in maintaining personal  
15 information (particularly sensitive personal information), and the value consumers place  
16 on keeping their PII secure.

17 37. Defendant owes duties to Plaintiff and the Class members to maintain  
18 adequate security and safeguards to protect the confidentiality of their PII.

19 38. Defendant owes a further duty to its customers to immediately and  
20 accurately notify them of a breach of its systems to protect them from identity theft and  
21 other misuse of their personal data and to take adequate measures to prevent further  
22 breaches.

23 ***The Categories of PII at Issue Here Are Particularly Valuable to Criminals***

24 39. Businesses that solicit, aggregate, and store sensitive PII are likely to be  
25 targeted by cyber criminals.

26 40. The FTC has released its updated publication on protecting PII for  
27  
28

1 businesses, which includes instructions on protecting PII, properly disposing of PII,  
2 understanding network vulnerabilities, implementing policies to correct security  
3 problems, using intrusion detection programs, monitoring data traffic, and having in place  
4 a response plan.

5  
6 41. The FTC has, upon information and belief, brought enforcement actions  
7 against businesses for failing to protect PII. The FTC has done this by treating a failure to  
8 employ reasonable measures to protect against unauthorized access to PII as a violation  
9 of the FTC Act, 15 U.S.C. § 45.

10  
11 42. General policy reasons support such an approach. A person whose personal  
12 information has been compromised may not see any signs of identity theft for *years*.  
13 According to a U.S. Government Accountability Office report:

14 [L]aw enforcement officials told us that in some cases, stolen data  
15 may be held for up to a year or more before being used to commit  
16 identity theft. Further, once stolen data have been sold or posted on  
17 the Web, fraudulent use of that information may continue for years.  
18 As a result, studies that attempt to measure the harm resulting from  
19 data breaches cannot necessarily rule out all future harm.<sup>5</sup>

20 43. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable  
21 commodity. A “cyber black-market” exists in which criminals openly post PII on a  
22 number of Internet websites. Plaintiff’s and Class members’ personal data that was stolen  
23 has a high value on both legitimate and black markets.

24 44. At an FTC public workshop in 2001, then-Commissioner Orson Swindle  
25 described the value of a consumer’s personal information as follows:

26 The use of third party information from public records, information  
27

28 <sup>5</sup> See <https://www.gao.gov/assets/gao-07-737.pdf> at 29 (last visited Sept. 20, 2022).

1 aggregators and even competitors for marketing has become a major  
2 facilitator of our retail economy. Even [Federal Reserve] Chairman  
3 [Alan] Greenspan suggested here some time ago that it's something  
4 on the order of the life blood, the free flow of information.<sup>6</sup>

5 45. Individuals rightfully place a high value not only on their PII, but also on  
6 the privacy of that data. Researchers have already begun to shed light on how much  
7 individuals value their data privacy—and the amount is considerable.

8 46. Notably, one study on website privacy determined that U.S. consumers  
9 valued the restriction of improper access to their personal information—the very injury at  
10 issue here—between \$11.33 and \$16.58 per website.<sup>7</sup> The study also determined that  
11 “[a]mong U.S. subjects, protection against errors, improper access, and secondary use of  
12 personal information is worth US\$30.49 – 44.62.”<sup>8</sup> This study was done in 2002. The  
13 sea-change in how pervasive the Internet is in everyday lives since then indicates that  
14 these values—when associated with the loss of PII to bad actors—would be exponentially  
15 higher today.

16 47. Identity thieves may commit various types of crimes such as immigration  
17 fraud, obtaining a driver's license or identification card in the victim's name but with  
18 another's picture, and/or using the victim's information to obtain a fraudulent tax refund  
19 or fraudulent unemployment benefits. The United States government and privacy experts  
20  
21  
22

23  
24 <sup>6</sup> FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging*  
25 *Consumer Data*, transcript, p. 8, available at [http://www.ftc.gov/news-events/events-](http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data)  
26 [calendar/2001/03/information-marketplace-merging-exchanging-consumer-data](http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data) (last visited  
27 Sept. 20. 2022).

28 <sup>7</sup> Hann, Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and*  
Singapore, at p. 17. Oct. 2002, available at [https://www.comp.nus.](https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf)  
edu.sg/~ipng/research/privacy. pdf (last visited Sept. 20. 2022).

<sup>8</sup> *Id.*

1 acknowledge that it may take years for identity theft to come to light and be detected.

2 48. To date, Defendant has offered Plaintiff and Class members only one year  
3 of credit monitoring and identity theft detection services. The offered service is wholly  
4 inadequate to protect Plaintiff and Class members from the threats they face for years to  
5 come, particularly in light of the PII at issue here, and is not an adequate cure of the Data  
6 Breach.  
7

8 49. The information Defendant allowed to be compromised and taken is of  
9 such that the harms to Plaintiff and the Class will continue to grow, and Plaintiff and  
10 Class members will continue to be at substantial risk for further imminent and future  
11 harm.  
12

### 13 *Damages from Data Breaches*

14 50. According to Javelin Strategy & Research, in 2017 alone over 16.7 million  
15 individuals were affected by identity theft, causing \$16.8 billion to be stolen.  
16

17 51. Consumers place a high value not only on their personal information, but  
18 also on the privacy of that data. This is because identity theft causes “significant negative  
19 financial impact on victims” as well as severe distress and other strong emotions and  
20 physical reactions.  
21

22 52. The United States Government Accountability Office explains that “[t]he  
23 term ‘identity theft’ is broad and encompasses many types of criminal activities,  
24 including fraud on existing accounts—such as unauthorized use of a stolen credit card  
25 number—or fraudulent creation of new accounts—such as using stolen data to open a  
26 credit card account in someone else’s name.” *See In re Zappos.com, Inc.*, 888 F.3d 1020,  
27  
28

1 1024 (9th Cir. 2018). The GAO Report notes that victims of identity theft will face  
2 “substantial costs and time to repair the damage to their good name and credit record.”

3 53. The FTC recommends that identity theft victims take several steps to  
4 protect their personal information after a data breach, including contacting one of the  
5 credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years  
6 if someone steals their identity), reviewing their credit reports often, contacting  
7 companies to remove fraudulent charges from their accounts, placing a credit freeze on  
8 their credit, and correcting their credit reports.  
9

10 54. Identity thieves use stolen personal information for “various types of  
11 criminal activities, such as when personal and financial is used to commit fraud or other  
12 crimes,” including “credit card fraud, phone or utilities fraud, bank fraud and government  
13 fraud.” *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data  
14 Breach can also be used to commit identity theft by placing Plaintiff and Class members  
15 at a higher risk of “phishing,” “vishing,” “smishing,” and “pharming,” which are which  
16 are ways for hackers to exploit information they already have to get even more personally  
17 identifying information through unsolicited email, text messages, and telephone calls  
18 purportedly from a legitimate company requesting personal, financial, and/or login  
19 credentials.  
20  
21

22 55. There may be a time lag between when harm occurs versus when it is  
23 discovered, and also between when personal information is stolen and when it is used.  
24 According to the U.S. Government Accountability Office, which conducted a study  
25 regarding data breaches:  
26  
27  
28



1 [L]aw enforcement officials told us that in some cases, stolen data  
2 may be held for up to a year or more before being used to commit  
3 identity theft. Further, once stolen data have been sold or posted on  
4 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.

5 *See* GAO Report, at p. 29.

6 56. Personal information is such a valuable commodity to identity thieves that  
7 once the information has been compromised, criminals often trade the information on the  
8 “cyber blackmarket” for years.  
9

10 57. Thus, there is a strong probability that entire batches of stolen information  
11 have been dumped on the black market, or are yet to be dumped on the black market,  
12 meaning Plaintiff and Class members are at an increased risk of fraud and identity theft  
13 for many years into the future.  
14

15 58. Data breaches are preventable. As Lucy Thompson wrote in the DATA  
16 BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches  
17 that occurred could have been prevented by proper planning and the correct design and  
18 implementation of appropriate security solutions.” She added that “[o]rganizations that  
19 collect, use, store, and share sensitive personal data must accept responsibility for  
20 protecting the information and ensuring that it is not compromised . . . .”  
21

22 59. “Most of the reported data breaches are a result of lax security and the  
23 failure to create or enforce appropriate security policies, rules, and procedures. . . .  
24 Appropriate information security controls, including encryption, must be implemented  
25 and enforced in a rigorous and disciplined manner so that a data breach never occurs.”  
26  
27  
28

1           60.     Indeed, here Defendant deployed enhanced security measures after the Data  
2 Breach, but should have implemented them to prevent the Data Breach.

3           61.     The types of information Defendant acknowledges were stolen by the  
4 criminals are sufficiently sensitive and valuable to identity thieves and criminals in  
5 perpetrating identity crimes. Defendant states that Plaintiff's and Class members' names,  
6 dates of birth, and driver's license or state identification numbers were taken in the Data  
7 Breach. This information can be used to perpetrate scams, victimize the persons who own  
8 the information, and commit identity theft and fraud.<sup>9</sup>

9  
10           62.     A person's driver's license or state identification numbers can be used  
11 alone or in conjunction with other pieces of information to commit serious fraud. *See*  
12 <https://www.aura.com/learn/can-someone-steal-your-identity-with-your-id> (last visited  
13 Sept. 19, 2022). For example, a driver's license number can be (a) sold on the Dark Web,  
14 (b) used to commit driver's license fraud, (c) used to create fake IDs using the stolen  
15 driver's license or identification number, (d) used to create synthetic identities, (e) used  
16 driver's license or identification number, (d) used to create synthetic identities, (e) used  
17 to commit identity theft, and (f) used to commit mail fraud. *Id.*

18  
19           63.     Criminals can use the information to devise and employ phishing and social  
20 engineering schemes capitalizing on the genuine information stolen from Defendant to  
21 send fraudulent mail and other communications to Plaintiff and Class members that look  
22 authentic, but which are designed to lure them into paying money or providing other  
23 information that the criminals can use to steal money.  
24  
25

26 \_\_\_\_\_  
27 <sup>9</sup> *See* <https://www.aura.com/learn/can-someone-steal-your-identity-with-your-id> (last visited  
28 Sept. 19, 2022).

1  
2 64. It is recommended that if your driver's license numbers is stolen, you  
3 should request a copy of your official driving record from the motor vehicles department  
4 and do it again at a later date.<sup>10</sup> Thieves may create a fake license using the stolen  
5 driver's license number and present it as identification during a traffic stop.<sup>11</sup>  
6

7 65. It is also recommended that if your driver's license or identification number  
8 is stolen, you should run a background check on yourself to see if there are any criminal  
9 convictions or arrest warrants that do not apply to you because these are a sign that  
10 someone has been using your identity. *Id.*  
11

12 ***Plaintiff Received Defendant's Data Breach Notification Letter***

13 66. In 2022, Plaintiff entered into a rental contract with U-Haul in Hamilton,  
14 Ohio, for a box truck, which she needed to move some large items.  
15

16 67. Plaintiff and Class members provided Defendant with significant personal  
17 information, including their names and birth dates, in conjunction with their driver's  
18 license and identification numbers.

19 68. Plaintiff provided Defendant with her driver's license for review when she  
20 entered into the rental contract for the box truck.  
21

22 69. Defendant has admitted that this information relating to Plaintiff and Class  
23 members was exposed, compromised, accessed, viewed without authorization, and stolen  
24 in the Data Breach by criminals.  
25

26 \_\_\_\_\_  
27 <sup>10</sup> See <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/> (last visited Sept. 19, 2022).

28 <sup>11</sup> *Id.*

1           70. On or about September 9, 2022, Defendant sent the Data Breach Notice by  
2 email notifying Plaintiff and Class members that PII—including their names, and driver’s  
3 license and identification numbers—was taken by an “unauthorized person” in the Data  
4 Breach. See **Exhibit 1**. Defendant omitted from its Data Breach Notice that Plaintiff’s  
5 and Class members’ birth dates were also taken by criminals in the Data Breach, but  
6 Defendant admitted that their birth dates were taken in its SEC Form 8-K Report.  
7

8  
9                                   ***Plaintiff’s and Class Members’ Damages***

10           71. As a direct and proximate result of Defendant’s conduct, Plaintiff and Class  
11 members have been placed at an imminent, immediate, and continuing increased risk of  
12 harm from fraud and identity theft.

13           72. Plaintiff and Class members have or will suffer actual injury as a direct  
14 result of the Data Breach including:  
15

- 16                   a) Spending time reviewing charges for any fraudulent charges and  
17 remedying any fraudulent charges found;
- 18                   b) Purchasing credit monitoring and identity theft prevention;
- 19                   c) Requesting their official driving record from the motor vehicles  
20 department and reviewing it for reports of traffic stops unrelated to  
21 themselves;
- 22                   d) Running a background check on themselves to see if there are any  
23 criminal convictions or arrest warrants that don't apply to them;
- 24                   e) Time and money addressing and remedying identity theft;
- 25                   f) Spending time placing “freezes” and “alerts” with credit reporting  
26 agencies and, subsequently, temporarily lifting a security freeze on a  
27 credit report, or removing a security freeze from a credit report;
- 28                   g) Spending time on the phone with or visiting financial institutions to  
dispute fraudulent charges;

- 1           h)     Contacting their financial institutions and closing or modifying
- 2                 financial accounts compromised as a result of the Data Breach; and
- 3           i)     Closely reviewing and monitoring bank accounts and credit reports
- 4                 for unauthorized activity for years to come.

5           73.     Moreover, Plaintiff and the Class members have an interest in ensuring that

6                 their personal information is protected from further breaches by the implementation of

7                 security measures and safeguards, including making sure that the storage of data

8                 containing their personal information is secure.

9           74.     As a direct and proximate result of Defendant's actions and inactions,

10                Plaintiff and Class members have suffered anxiety, emotional distress, and loss of

11                privacy.

12           75.     As a direct and proximate result of Defendant's actions and inactions,

13                Plaintiff and Class members are at an increased and immediate risk of future harm,

14                including from identity theft and fraud.

15           76.     As a result of the Data Breach, Plaintiff and Class members are at an

16                imminent risk of identity theft and fraud. This risk will continue to exist for years to

17                come, as Plaintiff and Class members must spend their time being extra vigilant, due to

18                Defendant's failures, to try to prevent being victimized for the rest of their lives.

19           77.     Because Defendant presented such an easy target to cyber criminals,

20                Plaintiff and Class members have already been subjected to violations of their privacy,

21                and have been exposed to a heightened and imminent risk of fraud and identity theft.

22                Plaintiff and Class members must now and in the future, spend time to more closely

23                monitor their affected PII to guard against identity theft and other fraud.

24           78.     Plaintiff and Class members may also incur out-of-pocket costs for, among

25

26

27

28

1 other things, purchasing credit monitoring services or other protective measures (such as  
2 obtaining their official traffic record and running a background check) to deter and detect  
3 identity theft.

4 **CLASS ACTION ALLEGATIONS**

5  
6 79. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23 on behalf of a  
7 class of similarly situated individuals (the “Class”) defined as follows:

8 All individuals in the United States whose personally identifiable  
9 information was accessed in the Data Breach announced by U-Haul  
10 International, Inc.

11 80. Excluded from the Class are Defendant; any entity in which Defendant has  
12 a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and  
13 the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and  
14 assigns of Defendant. Also excluded are the judges and court personnel in this case and  
15 any members of their immediate families.

16  
17 81. Plaintiff reserves the right to modify and/or amend the Class definition,  
18 including but not limited to creating subclasses, as necessary.

19 82. **Numerosity.** The Class is so numerous that joinder of all members is  
20 impracticable. The identities of all Class members are ascertainable through Defendant’s  
21 records.

22  
23 83. **Commonality.** There are numerous questions of law and fact common to  
24 Plaintiff and the Class, including the following:

- 25
- 26 ● Whether and to what extent Defendant had a duty to protect the PII  
of Plaintiff and Class members;
  - 27 ● Whether Defendant had a duty not to disclose the PII of Plaintiff and  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Class members to unauthorized third parties;

- Whether Defendant had a duty not to use the PII of Plaintiff and Class members for non-business purposes;
- Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class members;
- When Defendant actually learned of the Data Breach;
- Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised;
- Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII had been compromised;
- 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;
- Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- Whether Defendant violated the Drivers Privacy Protection Act by failing to adequately safeguard and protect the PII of Plaintiff and Class members thereby allowing the PII to be used for an impermissible purpose;
- Whether Plaintiff and Class members are entitled to actual damages, statutory damages, nominal damages, and/or exemplary damages as a result of Defendant’s wrongful conduct;
- Whether Plaintiff and Class members are entitled to restitution as a result of Defendant’s wrongful conduct; and
- Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

84. **Typicality.** Plaintiff’s claims are typical of the claims of the Class because Plaintiff, like all Class members, had her PII compromised, breached and stolen in the Data Breach. Plaintiff and Class members were injured through Defendant’s uniform misconduct described in this Complaint and assert the same claims for relief.

1           85.    **Adequacy.** Plaintiff and her counsel will fairly and adequately protect the  
2 interests of the Class. Plaintiff has retained counsel who are experienced in class actions  
3 and complex litigation, including data privacy litigation of this kind. Plaintiff has no  
4 interests that are antagonistic to, or in conflict with, the interests of other members of the  
5 Class.  
6

7           86.    **Predominance.** The questions of law and fact common to Class members  
8 predominate over any questions which may affect only individual members.  
9

10           87.    **Superiority.** A class action is superior to other available methods for the  
11 fair and efficient adjudication of the controversy. Class treatment of common questions  
12 of law and fact is superior to multiple individual actions or piecemeal litigation.  
13 Moreover, absent a class action, most Class members would find the cost of litigating  
14 their claims prohibitively high and would therefore have no effective remedy, so that in  
15 the absence of class treatment, Defendant's violations of law inflicting substantial  
16 damages in the aggregate would go unremedied without certification of the Class.  
17 Plaintiff and Class members have been harmed by Defendant's wrongful conduct and/or  
18 action.  
19

20           88.    Litigating this action as a class action will reduce the possibility of  
21 repetitious litigation relating to Defendant's conduct and/or inaction. No difficulties  
22 would be encountered in this litigation that would preclude its maintenance as a class  
23 action.  
24

25           89.    Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3),  
26 because the above common questions of law or fact predominate over any questions  
27  
28



1 affecting individual members of the Class, and a class action is superior to other available  
2 methods for the fair and efficient adjudication of this controversy.

3 90. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2),  
4 because Defendant has acted or refused to act on grounds that apply generally to the  
5 Classes so that final injunctive relief or corresponding declaratory relief is appropriate  
6 respecting the Class as a whole.  
7

8 **COUNT I**  
9 **Negligence**  
10 ***(On behalf of Plaintiff and the Class)***

11 91. Plaintiff repeats and realleges the allegations of the paragraphs 1-90 with  
12 the same force and effect as though fully set forth herein.

13 92. Defendant's actions and inactions were of the type that would result in  
14 foreseeable, unreasonable risk of harm to Plaintiff and Class members. Defendant knew,  
15 or should have known, of the risks inherent in collecting and storing the personal  
16 information of Plaintiff and Class members and the importance of adequate security in  
17 storing the information. Additionally, Defendant is aware of numerous, well-publicized  
18 data breaches that exposed the personal information of individuals.  
19

20 93. Defendant had a common law duty to prevent foreseeable harm to  
21 Plaintiff's and Class members' PII. This duty existed because Plaintiff and Class  
22 members were the foreseeable and probable victims of the failure of Defendant to adopt,  
23 implement, and maintain reasonable security measures so that Plaintiff's and Class  
24 members' personal information would not be unsecured and accessible by unauthorized  
25 persons.  
26  
27  
28

1           94. Defendant had a special relationship with Plaintiff and Class members.  
2 Defendant was entrusted with Plaintiff’s and Class members’ personal information, and  
3 Defendant was in a position to protect the personal information from unauthorized  
4 access.

5           95. The duties of Defendant also arose under section 5 of the FTC Act, which  
6 prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and  
7 enforced by the FTC, the unfair practice of failing to use reasonable measures to protect  
8 individuals’ personal information by companies. Various FTC publications and data  
9 security breach orders further form the basis of the duties of Defendant.  
10

11           96. Defendant had a duty to exercise reasonable care in obtaining, retaining,  
12 securing, safeguarding, deleting, and protecting Plaintiff’s and Class members’ personal  
13 information in its possession so that the personal information would not come within the  
14 possession, access, or control of unauthorized persons.  
15

16           97. More specifically, the duties of Defendant included, among other things,  
17 the following duties, and Defendant carelessly and negligently acted or failed to act in  
18 one or more of the following ways:  
19

- 20
- 21           ● Failing to conduct proper and reasonable due diligence over its data  
22 security systems, practices, and procedures;
  - 23           ● Failing to adopt, implement, and maintain adequate security  
24 measures for protecting an individual’s personal information to  
25 ensure that the information is not accessible online by unauthorized  
26 persons;
  - 27           ● Failing to adopt, implement, and maintain adequate security  
28 measures for deleting or destroying personal information when  
Defendant’s business needs no longer required such information to  
be stored and maintained; and

- Failing to adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

1  
2  
3  
4 98. Defendant breached the foregoing duties to exercise reasonable care in  
5 obtaining, retaining, securing, safeguarding, deleting, and protecting personal information  
6 in its possession so that the information would not come within the possession, access, or  
7 control of unauthorized persons.  
8

9 99. Defendant acted with reckless disregard for the security of the personal  
10 information of Plaintiff and Class members because Defendant knew or should have  
11 known that its data security was not adequate to safeguard the personal information that  
12 was collected and stored.  
13

14 100. Defendant acted with reckless disregard for the rights of Plaintiff and the  
15 Class members by failing to promptly detect the Data Breach, and further, by failing to  
16 notify Plaintiff and the Class members of the Data Breach in the most expedient time  
17 possible and without unreasonable delay pursuant to common law duties to provide  
18 reasonably timely and truthful data-breach notification, so that Plaintiff and Class  
19 members could promptly take measures to protect themselves from the consequences of  
20 the unauthorized access to the personal information compromised in the Data Breach.  
21  
22

23 101. As a result of the conduct of Defendant, Plaintiff and Class members have  
24 suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have  
25 suffered actual damages including, but not limited to, imminent risk of identity theft;  
26 expenses and/or time spent on credit monitoring for a period of years; time spent  
27  
28

1 obtaining and reviewing background checks to see if there are any criminal convictions  
2 or arrest warrants that do not apply to themselves; time spent obtaining official driving  
3 records from the motor vehicles department to review and see if there are any reports of  
4 traffic stops that do not apply to themselves; scrutinizing bank statements, credit card  
5 statements, and credit reports; time spent initiating fraud alerts and credit freezes and  
6 subsequently temporarily lifting credit freezes; and increased risk of future harm. Further,  
7 Plaintiff and Class members have suffered and will continue to suffer other forms of  
8 injury and/or harm including, but not limited to, anxiety, emotional distress, loss of  
9 privacy, and other economic and non-economic losses.  
10

11  
12 **COUNT II**  
13 **Negligence Per Se**  
14 ***(On Behalf of Plaintiff and the Class)***

15 102. Plaintiff repeats and realleges the allegations of paragraphs 1-90 with the  
16 same force and effect as though fully set forth herein.

17 103. “Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates  
18 enforceable duties, and this duty is ascertainable as it relates to data breach cases based  
19 on the text of the statute and a body of precedent interpreting the statute and applying it  
20 to the data beach context.” *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F.  
21 Supp. 3d 374, 407 (E.D. Va. 2020). “For example, in *F.T.C. v. Wyndham Worldwide*  
22 *Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third  
23 Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach  
24 cases.” *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.  
25  
26

27 104. Plaintiff's and Class members' PII was and is nonpublic personal  
28

1 information and customer information.

2 105. Plaintiff and Class members are in the group of persons the FTC Act was  
3 enacted and implemented to protect, and the harms they suffered in the Data Breach as a  
4 result of Defendant's violations of the FTC Act were the types of harm they were  
5 designed to prevent.  
6

7 106. As a result of the conduct of Defendant that violated the FTC Act, Plaintiff  
8 and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff  
9 and Class members have suffered actual damages including, but not limited to, imminent  
10 risk of identity theft; expenses and/or time spent on credit monitoring for a period of  
11 years; time spent obtaining and reviewing background checks to see if there are any  
12 criminal convictions or arrest warrants that do not apply to themselves; time spent  
13 obtaining official driving records from the motor vehicles department to see if there are  
14 any reports of traffic stops that do not apply to themselves; scrutinizing bank statements,  
15 credit card statements, and credit reports; time spent initiating fraud alerts and credit  
16 freezes and subsequently temporarily lifting credit freezes; and increased risk of future  
17 harm. Further, Plaintiff and Class members have suffered and will continue to suffer  
18 other forms of injury and/or harm including, but not limited to, anxiety, emotional  
19 distress, loss of privacy, and other economic and non-economic losses.  
20  
21  
22

23 **COUNT III**  
24 **Breach of Implied Contract**  
25 ***(On Behalf of Plaintiff and the Class)***

26 107. Plaintiff repeats and realleges the allegations of paragraphs 1-90 with the  
27 same force and effect as though fully set forth herein.  
28

1 108. Defendant acquired and maintained the PII of Plaintiff and Class members.

2 109. At the time Defendant acquired the PII of Plaintiff and Class members,  
3 there was a meeting of the minds and a mutual understanding that Defendant would  
4 safeguard the PII using reasonable security measures and not take unjustified risks when  
5 collecting, digitizing, and storing the PII.  
6

7 110. Plaintiff and Class members would not have entrusted their PII to  
8 Defendant had they known that Defendant would make the PII vulnerable and fail to take  
9 reasonable precautions, such as encrypting the data while in storage, and deleting PII that  
10 was no longer necessary.  
11

12 111. Defendant promised to comply with industry standards and to ensure that  
13 Plaintiff's and Class members' PII would remain protected.

14 112. Implicit in the agreements between Plaintiff and Class members and  
15 Defendant to provide PII was Defendant's obligation to:  
16

- 17 ● Use the PII for business purposes only;
- 18 ● Take reasonable steps to protect and safeguard the PII from known  
19 and foreseeable risks;
- 20 ● Prevent unauthorized disclosures of the PII;
- 21 ● Provide Plaintiff and Class members with prompt and sufficient  
22 notice of instances where unauthorized access to the PII is  
23 reasonably suspected; and
- 24 ● Reasonably safeguard and protect the PII of Plaintiff and Class  
25 members from unauthorized disclosures or uses.  
26  
27  
28

1           113. In collecting and maintaining the PII of Plaintiff and Class members and  
2 publishing and disseminating privacy notices, Defendant entered into contracts to protect  
3 and keep security over the PII of Plaintiff and Class members.

4           114. Plaintiff and Class members fully performed under their contract with  
5 Defendant.  
6

7           115. Defendant breached the contracts by failing to protect and keep private the  
8 personal information of Plaintiff and Class members, including by failing to: (i) encrypt  
9 or tokenize the sensitive PII of Plaintiff and Class members, (ii) delete such PII that  
10 Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of  
11 the PII from the Internet where such accessibility was not justified, and (iv) otherwise  
12 review and improve the security of the network system that contained such PII.  
13

14           116. Defendant also breached a duty to provide reasonably expedient and  
15 sufficient notification of the Data Breach.  
16

17           117. As a result of Defendant's breach of implied contract, Plaintiff and Class  
18 members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class  
19 members have suffered actual damages including, but not limited to, imminent risk of  
20 identity theft; expenses and/or time spent on credit monitoring for a period of years; time  
21 spent obtaining and reviewing background checks to see if there are any criminal  
22 convictions or arrest warrants that do not apply to themselves; time spent obtaining  
23 official driving records from the motor vehicles department to see if there are any reports  
24 of traffic stops that do not apply to themselves; scrutinizing bank statements, credit card  
25 statements, and credit reports; time spent initiating fraud alerts and credit freezes and  
26  
27  
28

1 subsequently temporarily lifting credit freezes; and increased risk of future harm. Further,  
2 Plaintiff and Class members have suffered and will continue to suffer other forms of  
3 injury and/or harm including, but not limited to, anxiety, emotional distress, loss of  
4 privacy, and other economic and non-economic losses.

5  
6 **COUNT IV**

7 **Violations of the Drivers Privacy Protection Act, 18 U.S.C. § 2721, *et seq.***  
8 ***(On Behalf of Plaintiff and the Class)***

9 118. Plaintiff repeats and realleges the allegations of paragraphs 1-90 with the  
10 same force and effect as though fully set forth herein.

11 119. A “‘motor vehicle record’ means any record that pertains to a motor vehicle  
12 operator's permit, motor vehicle title, motor vehicle registration, or identification card  
13 issued by a department of motor vehicles.” *See* 18 U.S.C. § 2725(1).

14 120. “Personal information” means “information that identifies an individual”,  
15 including, but not limited to, an individual’s driver’s identification number. *See* 18 U.S.C.  
16 § 2725(3).

17 121. Defendant knowingly obtained Plaintiff’s and Class members’ personal  
18 information from a motor vehicle record, including their names and driver’s license or  
19 state identification numbers.

20 122. Defendant populated its customer contract search tool with Plaintiff’s and  
21 Class members’ personal information, including their driver’s license or state  
22 identification numbers.

23 123. Defendant reasonably should have known that populating its customer  
24 contract search tool with Plaintiff’s and Class members’ driver’s license and  
25



1 identification numbers without adequate security and safeguards would result in  
2 disclosure of the personal information to cybercriminals for impermissible purposes.

3 124. Because Defendant failed to implement adequate security and safeguards to  
4 prevent the Data Breach, Plaintiff's and Class members' driver's license and  
5 identification numbers were disclosed to cybercriminals for impermissible purposes.  
6

7 125. Plaintiff and each Class member demands actual damages, but not less than  
8 liquidated damages in the amount of \$2,500, punitive damages upon proof of willful or  
9 reckless disregard of the law, reasonable attorney's fees and other litigation costs  
10 reasonably incurred, and such other preliminary and equitable relief as the Court  
11 determines to be appropriate.  
12

13 **PRAYER FOR RELIEF**

14 WHEREFORE Plaintiff, individually and on behalf of the Class, requests that the  
15 Court:  
16

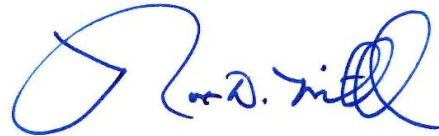
- 17 A. Certify this case as a class action on behalf of the Class defined  
18 above, appoint Plaintiff as the Class representative, and appoint the  
19 undersigned counsel as Class counsel;
- 20 B. Award declaratory, injunctive and other equitable relief as is  
21 necessary to protect the interests of Plaintiff and Class members;
- 22 C. Award restitution and damages to Plaintiff and Class members in an  
23 amount to be determined at trial;
- 24 D. Award Plaintiff and Class members their reasonable litigation  
25 expenses and attorneys' fees to the extent allowed by law;
- 26 E. Award Plaintiff and Class members pre- and post-judgment interest,  
27 to the extent allowable; and
- 28 F. Award such other and further relief as equity and justice may  
require.

**DEMAND FOR JURY TRIAL**

1  
2 Plaintiff demands a trial by jury of any and all issues in this action so triable of  
3  
4 right.

5 RESPECTFULLY SUBMITTED this 29th day of September, 2022.

6 Plaintiff SANDRA BROWN, individually and on  
7 behalf of all others similarly situated,

8 

9  
10 By: \_\_\_\_\_

11 Marc E. Dann (*pro hac vice* anticipated)

12 Brian D. Flick (*pro hac vice* anticipated)

13 **DannLaw**

14 15000 Madison Avenue

15 Lakewood, OH 44107

16 Emails: mdann@dannlaw.com;

17 notices@dannlaw.com

18 Thomas A. Zimmerman, Jr. (*pro hac vice*  
19 anticipated)

20 Sharon A. Harris (*pro hac vice* anticipated)

21 **Zimmerman Law Offices, P.C.**

22 77 W. Washington Street, Suite 1220

23 Chicago, Illinois 60602

24 Email: firm@attorneyzim.com

25 Robert D. Mitchell

26 Christopher J. Waznik

27 Anne P. Barber

28 CM Matthew Luk



**TIFFANY & BOSCO**  
P.A.

Camelback Esplanade II, Seventh Floor

2525 East Camelback Road

Phoenix, Arizona 85016

E-mails: rdm@tblaw.com; cjw@tblaw.com;

apb@tblaw.com; cml@tblaw.com

*Counsel for Plaintiff and the Class*