

1 Alex R. Straus (SBN 321366)
2 astraus@milberg.com
3 **MILBERG COLEMAN BRYSON**
4 **PHILLIPS GROSSMAN, PLLC**
5 280 S. Beverly Drive
6 Beverly Hills, CA 90212
7 T: 917-471-1894
8 F: 865-522-0049

9 *Attorneys for Plaintiff*

10 **UNITED STATES DISTRICT COURT**
11 **CENTRAL DISTRICT OF CALIFORNIA**

12 JORDAN EASLEY, individually and on
13 behalf of all others similarly situated,

14 Plaintiffs,

15 v.

16 UTILITY TRAILER
17 MANUFACTURING COMPANY,

18 Defendant.

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

19 Plaintiff JORDAN EASLEY (“Plaintiff”), individually and on behalf of all
20 others similarly situated, brings this action against Defendant UTILITY TRAILER
21 MANUFACTURING COMPANY, (“UTM” or “Defendant”), to obtain damages,
22 restitution, and injunctive relief for the Class, as defined below, from Defendant.
23 Plaintiff makes the following allegations upon information and belief, except as to
24
25
26
27
28

1 his own actions, the investigation of his counsel, and the facts that are a matter of
2 public record:

3
4 **NATURE OF THE ACTION**

5 1. This class action arises out of the recent targeted cyber-attack against
6 Defendant UTM that allowed a third party to access Defendant UTM’s computer
7 systems and data, resulting in the compromise of highly sensitive personal
8 information belonging to tens of thousands of current and former employees and
9 their family members (the “Cyber-Attack”).
10

11
12 2. As a result of the Cyber-Attack, Plaintiff and Class Members suffered
13 ascertainable injury and damages in the form of the substantial and present risk of
14 fraud and identity theft from their unlawfully accessed and compromised private
15 and confidential information (including Social Security numbers), lost value of their
16 private and confidential information, out-of-pocket expenses and the value of their
17 time reasonably incurred to remedy or mitigate the effects of the attack.
18
19

20 3. Plaintiff’s and approximately 28,703 Class Members’ sensitive
21 personal information—which was entrusted to Defendant, their officials and
22 agents—was compromised, unlawfully accessed, and stolen due to the Cyber-
23 Attack and subsequent data breach (the “Data Breach”). Information compromised
24 in the Cyber-Attack includes at least the following: full names and Social Security
25 numbers (collectively the “Private Information”).
26
27
28

1 4. Plaintiff brings this class action lawsuit on behalf of all those similarly
2 situated to address Defendant’s inadequate safeguarding of Class Members’ Private
3 Information that it collected and maintained.
4

5 5. Defendant maintained the Private Information in a reckless manner. In
6 particular, the Private Information was maintained on Defendant UTM’s computer
7 network in a condition vulnerable to cyber-attacks of this type.
8

9 6. Upon information and belief, the mechanism of the Cyber-Attack and
10 potential for improper disclosure of Plaintiff’s and Class Members’ Private
11 Information was a known and foreseeable risk to Defendant, and Defendant was on
12 notice that failing to take steps necessary to secure the Private Information from
13 those risks left that property in a dangerous condition.
14

15 7. In addition, Defendant and its employees failed to properly monitor
16 the computer network and systems that housed the Private Information. The Cyber-
17 Attack occurred in April 2021 but was not discovered until November 23, 2021.
18 Had Defendant properly monitored their property, they would have discovered the
19 intrusion sooner.
20

21 8. Plaintiff’s and Class Members’ identities are now at risk because of
22 Defendant’s negligent conduct since the Private Information that Defendant
23 collected and maintained is now in the hands of data thieves.
24

25 9. Armed with the Private Information accessed in the Cyber-Attack, data
26
27
28

1 thieves can commit a variety of crimes including, *e.g.*, opening new financial
2 accounts in Class Members' names, taking out loans in Class Members' names,
3 using Class Members' names to obtain medical services, using Class Members'
4 health information to target other phishing and hacking intrusions based on their
5 individual health needs, using Class Members' information to obtain government
6 benefits, filing fraudulent tax returns using Class Members' information, obtaining
7 driver's licenses in Class Members' names but with another person's photograph,
8 and giving false information to police during an arrest.

11
12 10. As a further result of the Cyber-Attack, Plaintiff and Class Members
13 have been exposed to a substantial and present risk of fraud and identity theft.
14 Plaintiff and Class Members must now and in the future closely monitor their
15 financial accounts to guard against identity theft.

17 11. Plaintiff and Class Members have and may also incur out of pocket
18 costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports,
19 or other protective measures to deter and detect identity theft.

21 12. As a direct and proximate result of the Cyber-Attack and subsequent
22 Data Breach, Plaintiff and Class Members have suffered and will continue to suffer
23 damages and economic losses in the form of: 1) the loss of time needed to take
24 appropriate measures to avoid unauthorized and fraudulent charges; change their
25 usernames and passwords on their accounts; investigate, correct and resolve
26
27
28

1 unauthorized debits; deal with spam messages and e-mails received subsequent to
2 the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiff
3 and Class Members have likewise suffered and will continue to suffer an invasion
4 of their property interest in their own personally identifying information (“PII”)
5 such that they are entitled to damages for unauthorized access to and misuse of their
6 PII from Defendant, and Plaintiff and Class Members will suffer from future
7 damages associated with the unauthorized use and misuse of their PII as thieves will
8 continue to use the stolen information to obtain money and credit in their name for
9 several years.
10
11
12

13 13. Plaintiff seeks to remedy these harms on behalf of themselves and all
14 similarly situated individuals whose Private Information was accessed and/or
15 removed from the network during the Cyber-Attack.
16

17 14. Plaintiff seeks remedies including, but not limited to, compensatory
18 damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive
19 relief including improvements to Defendant’s data security systems, future annual
20 audits, and adequate credit monitoring services funded by Defendant.
21

22 15. Accordingly, Plaintiff brings this action against Defendant seeking
23 redress for their unlawful conduct asserting claims for negligence, negligence *per*
24 *se*, breach of implied contract, and violation of the consumer protection statutes
25 invoked herein.
26
27
28

1 **PARTIES**

2 16. Plaintiff Jordan Easley is an individual citizen of the State of Arkansas
3 residing in Marmaduke, Arkansas. Plaintiff Easley began employment with UTM
4 in or around the fall of 2017 as an assembler. As a condition of employment with
5 UTM, he was required to provide his Private Information. On or about February 11,
6 2022, Plaintiff Easley received notice from Defendant that the Data Breach had
7 occurred following a “suspicious activity impacting [UTM’s] computer systems,”
8 and that his personal data (including his name, address and Social Security number)
9 was involved.
10
11
12

13 17. Defendant UTM (“UTM”) is a California corporation with its principal
14 place of 17295 Railroad Street, Suite A, City of Industry, California, 91748.
15

16 **JURISDICTION AND VENUE**

17 18. This Court has subject matter jurisdiction over this action under the
18 Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy
19 exceeds \$5 million, exclusive of interest and costs. Upon information and belief,
20 the number of class members is in the tens of thousands, many of whom have
21 different citizenship from Defendant, including the named Plaintiff here. Thus,
22 minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).
23
24

25 19. This Court has jurisdiction over the Defendant because it operates
26 and/or is incorporated in this District, and the computer systems implicated in this
27
28

1 Data Breach are likely based in this District.

2 20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1)
3 because a substantial part of the events giving rise to this action occurred in this
4 District. Defendant is based in this District, maintains Class Members' PII and
5 protected health information ("PHI") in the District and have caused harm to Class
6 Members residing in this District.
7
8

9 **FACTUAL ALLEGATIONS**

10 ***Defendant's Business***

11
12 21. Defendant UTM is an semi truck dry van, flatbed, and refrigerated van
13 trailer manufacturing company, based in the City of Industry, Los Angeles County,
14 California.
15

16 22. Defendant designs and manufactures dry freight and refrigerated
17 freight vans, flatbed trailers, and Tautliner curtain-sided trailers.
18

19 23. UTM operates five factories. Refrigerated trailers are made in Marion,
20 Virginia, and in the Freeport Center in Clearfield, Utah. Dry vans are produced in
21 Glade Spring, Virginia and Paragould, Arkansas. Flatbed trailers and Tautliners are
22 made in Enterprise, Alabama.
23

24 24. In the ordinary course of doing business with Defendant, current and
25 former employees provide Defendant with sensitive, personal and private
26 information such as:
27
28

- 1 • Name;
- 2 • Address;
- 3 • Phone number;
- 4 • Driver's license number;
- 5 • Social Security number;
- 6 • Date of birth;
- 7 • Email address;
- 8 • Gender.

9
10
11
12 25. On information and belief, in the course of collecting Private
13 Information from current and former employees, including Plaintiff, Defendant
14 promised to provide confidentiality and adequate security for employee data
15 through their applicable privacy policy and through other disclosures.
16
17

18 26. Plaintiff and Class Members, as current and former employees, relied
19 on the Defendant to keep their PII confidential and securely maintained, to use this
20 information for business purposes only, and to make only authorized disclosures of
21 this information. Plaintiff and Class Members demand security to safeguard their
22 PII.
23

24
25 27. Defendant had a duty to adopt reasonable measures to protect the PII
26 of Plaintiff and Class Members from involuntary disclosure to third parties.
27
28

The Cyber-Attack and Data Breach

1
2
3 28. On or about February 11, 2022, Defendant UTM began notifying
4 current and former employees, and state Attorneys General about a data breach that
5 occurred on or about April 25, 2021 (the “Data Breach”).
6

7 29. According to the Notice of Data Breach letters, and letters sent to state
8 Attorneys General, UTM’s security team, UTM “became aware of suspicious
9 activity impacting [UTM’s] computer systems” on or about April 25, 2021, and that
10 an “unknown actor may have viewed and taken certain information during a period
11 of unauthorized access on [UTM’s] computer systems between approximately April
12 5 and 25, 2021.”
13
14

15 30. Incredibly, the cyberthieves had unfettered access to Defendant’s
16 computer systems for 20 days without Defendant’s knowledge.
17

18 31. Even worse, Defendant did not discover the Data Breach until seven
19 (7) months later.

20 32. Plaintiff Easley was informed that his full name, address, and Social
21 Security number were among the data “taken” in the Data Breach.
22

23 33. Due to the severity of the Data Breach, Defendant offered consumers
24 “twelve (12) months of complimentary access to credit monitoring and identity
25 restoration services through Experience.”
26

27 34. Based on the Notice of Data Breach letter he received, which informed
28

1 Plaintiff that his Private Information was accessed and “taken” on Defendant’s
2 network and computer systems, Plaintiff believes his name, address, and Social
3 Security number were stolen from Defendant’s network and subsequently sold on
4 the Dark Web.
5

6 35. Defendant had obligations created by contract, industry standards,
7 common law, and representations made to Plaintiff and Class Members, to keep
8 their Private Information confidential and to protect it from unauthorized access and
9 disclosure.
10

11 36. Plaintiff and Class Members provided their Private Information to
12 Defendant with the reasonable expectation and mutual understanding that
13 Defendant would comply with its obligations to keep such information confidential
14 and secure from unauthorized access.
15

16 37. Defendant’s data security obligations were particularly important
17 given the substantial increase in cyber-attacks and/or data breaches preceding the
18 date of the breach.
19

20 38. In 2019, a record 1,473 data breaches occurred, resulting in
21 approximately 164,683,455 sensitive records being exposed, a 17% increase from
22 2018.¹
23
24

25
26
27 ¹ [https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-
28 Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf) (last accessed Dec. 10, 2020).

1 amounts of data being transmitted from the system; and have a response plan ready
2 in the event of a breach.

3
4 42. The FTC further recommends that companies not maintain PII longer
5 than is needed for authorization of a transaction; limit access to sensitive data;
6 require complex passwords to be used on networks; use industry-tested methods for
7 security; monitor for suspicious activity on the network; and verify that third-party
8 service providers have implemented reasonable security measures.
9

10
11 43. The FTC has brought enforcement actions against businesses for
12 failing to protect consumer data adequately and reasonably, treating the failure to
13 employ reasonable and appropriate measures to protect against unauthorized access
14 to confidential consumer data as an unfair act or practice prohibited by Section 5 of
15 the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting
16 from these actions further clarify the measures businesses must take to meet their
17 data security obligations.
18

19
20 44. Defendant failed to properly implement basic data security practices,
21 and their failure to employ reasonable and appropriate measures to protect against
22 unauthorized access to consumer PII constitutes an unfair act or practice prohibited
23 by Section 5 of the FTCA, 15 U.S.C. § 45.
24

25 45. Defendant was at all times fully aware of its obligation to protect the
26 Private Information of customers and prospective customers. Defendant was also
27

1 aware of the significant repercussions that would result from its failure to do so.

2 ***Defendant Fail to Comply with Industry Standards***

3
4 46. A number of industry and national best practices have been published
5 and should have been used as a go-to resource and authoritative guide when
6 developing Defendant's cybersecurity practices.

7
8 47. Best cybersecurity practices that are standard in the financial services
9 industry include installing appropriate malware detection software; monitoring and
10 limiting the network ports; protecting web browsers and email management
11 systems; setting up network systems such as firewalls, switches and routers;
12 monitoring and protection of physical security systems; protection against any
13 possible communication system; training staff regarding critical points.

14
15
16 48. Upon information and belief, Defendant failed to meet the minimum
17 standards of the following cybersecurity frameworks: the NIST Cybersecurity
18 Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-
19 4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-
20 3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for
21 Internet Security's Critical Security Controls (CIS CSC), which are established
22 standards in reasonable cybersecurity readiness.

23
24
25 49. These foregoing frameworks are existing and applicable industry
26 standards in Defendant's industry, and Defendant failed to comply with these
27

1 accepted standards, thereby opening the door to the Cyber-Attack and causing the
2 data breach.

3
4 ***Defendant's Breach***

5 50. Defendant breached its obligations to Plaintiff and Class Members
6 and/or was otherwise negligent and reckless because it failed to properly maintain
7 and safeguard its computer systems, networks, and data. Defendant's unlawful
8 conduct includes, but is not limited to, the following acts and/or omissions:
9

- 10
- 11 a. Failing to maintain an adequate data security system to reduce the
12 risk of data breaches and cyber-attacks;
 - 13 b. Failing to adequately protect current and former employees' Private
14 Information;
 - 15 c. Failing to adequately protect Private Information of current and
16 former employees' family members;
 - 17 d. Failing to properly monitor its own data security systems for
18 existing intrusions, brute-force attempts, and clearing of event logs;
 - 19 e. Failing to apply all available security updates;
 - 20 f. Failing to install the latest software patches, update its firewalls,
21 check user account privileges, or ensure proper security practices;
 - 22 g. Failing to practice the principle of least-privilege and maintain
23 credential hygiene;
 - 24
 - 25
 - 26
 - 27

- 1 h. Failing to avoid the use of domain-wide, admin-level service
- 2 accounts;
- 3
- 4 i. Failing to employ or enforce the use of strong randomized, just-in-
- 5 time local administrator passwords; and
- 6
- 7 j. Failing to properly train and supervise employees in the proper
- 8 handling of inbound emails.

9 51. As the result of computer systems in need of security upgrading and
10 inadequate procedures for handling cybersecurity threats, Defendant negligently
11 and unlawfully failed to safeguard Plaintiff’s and Class Members’ Private
12 Information.
13

14 ***Data Breaches Cause Disruption and Put Victims at an***
15 ***Increased Risk of Fraud and Identity Theft***
16

17 52. Defendant understood the Private Information it collected is highly
18 sensitive, and of significant value to those who would use it for wrongful purposes,
19 like the cyber-criminals who perpetrated this Cyber-Attack.
20

21 53. The United States Government Accountability Office released a report
22 in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of
23 identity theft will face “substantial costs and time to repair the damage to their good
24 name and credit record.”²
25

26
27 ² See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;
28 However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June

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

7
8
9 55. Identity thieves use stolen personal information such as Social Security
10 numbers for a variety of crimes, including credit card fraud, phone or utilities fraud,
11 and bank/finance fraud.
12

13 56. Identity thieves can also use Social Security numbers to obtain a
14 driver's license or official identification card in the victim's name but with the
15 thief's picture; use the victim's name and Social Security number to obtain
16 government benefits; or file a fraudulent tax return using the victim's information.
17

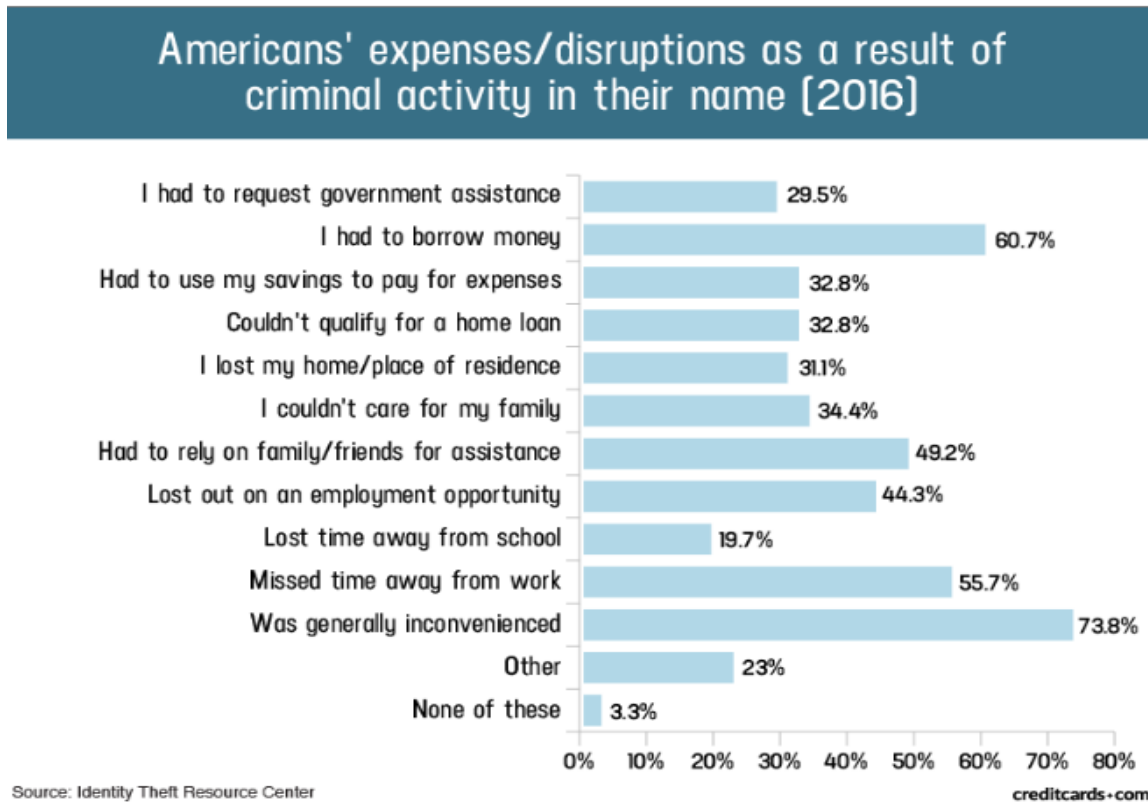
18 57. In addition, identity thieves may obtain a job using the victim's Social
19 Security number, rent a house or receive medical services in the victim's name, and
20 may even give the victim's personal information to police during an arrest resulting
21 in an arrest warrant being issued in the victim's name.
22

23
24 58. A study by Identity Theft Resource Center shows the multitude of
25

26 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Apr. 12, 2019) ("GAO
27 Report").

28 ³ See <https://www.identitytheft.gov/Steps> (last visited Dec. 8, 2020).

1 harms caused by fraudulent use of personal and financial information:⁴



17 59. What's more, theft of Private Information is also gravely serious. PII

18 is a valuable property right.⁵

19

20 60. Its value is axiomatic, considering the value of Big Data in corporate

21 America and the consequences of cyber thefts include heavy prison sentences. Even

22

23

24 ⁴ See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>

25 (last accessed Dec. 10, 2020).

26 ⁵ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable*

27 *Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-

28 4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

1 this obvious risk to reward analysis illustrates beyond doubt that Private
2 Information has considerable market value.

3
4 61. It must also be noted there may be a substantial time lag—measured in
5 years—between when harm occurs versus when it is discovered, and also between
6 when Private Information and/or financial information is stolen and when it is used.
7 According to the U.S. Government Accountability Office, which conducted a study
8 regarding data breaches:
9

10
11 [L]aw enforcement officials told us that in some cases, stolen data may
12 be held for up to a year or more before being used to commit identity
13 theft. Further, once stolen data have been sold or posted on the Web,
14 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.

15 *See* GAO Report at 29.

16
17 62. Private Information and financial information are such valuable
18 commodities to identity thieves that once the information has been compromised,
19 criminals often trade the information on the “cyber black-market” for years.

20
21 63. Indeed, a robust “cyber black market” exists in which criminals openly
22 post stolen Private Information on multiple underground Internet websites.

23
24 64. Where the most private information belonging to Plaintiffs and Class
25 Members was accessed and removed from Defendant’s network, and entire batches
26 of that stolen information already dumped by the cyberthieves on the cyber black
27 market, there is a strong probability that additional batches of stolen information
28

1 are yet to be dumped on the black market, meaning Plaintiffs and Class Members
2 are at an increased risk of fraud and identity theft for many years into the future.

3
4 65. Thus, Plaintiffs and Class Members must vigilantly monitor their
5 financial accounts for many years to come.

6
7 66. Sensitive information can sell for as much as \$363 according to the
8 Infosec Institute. PII is particularly valuable because criminals can use it to target
9 victims with frauds and scams. Once PII is stolen, fraudulent use of that information
10 and damage to victims may continue for years.

11
12 67. The PII of consumers remains of high value to criminals, as evidenced
13 by the prices they will pay through the dark web. Numerous sources cite dark web
14 pricing for stolen identity credentials. For example, personal information can be
15 sold at a price ranging from \$40 to \$200.

16
17 68. Social Security numbers are among the worst kind of personal
18 information to have stolen because they may be put to a variety of fraudulent uses
19 and are difficult for an individual to change. The Social Security Administration
20 stresses that the loss of an individual's Social Security number, as is the case here,
21 can lead to identity theft and extensive financial fraud.

22
23
24 69. For example, the Social Security Administration has warned that
25 identity thieves can use an individual's Social Security number to apply for
26 additional credit lines. Such fraud may go undetected until debt collection calls
27

1 commence months, or even years, later. Stolen Social Security Numbers also make
2 it possible for thieves to file fraudulent tax returns, file for unemployment benefits,
3 or apply for a job using a false identity. Each of these fraudulent activities is difficult
4 to detect. An individual may not know that his or her Social Security Number was
5 used to file for unemployment benefits until law enforcement notifies the
6 individual's employer of the suspected fraud. Fraudulent tax returns are typically
7 discovered only when an individual's authentic tax return is rejected.
8

9
10 70. Moreover, it is not an easy task to change or cancel a stolen Social
11 Security number. An individual cannot obtain a new Social Security number
12 without significant paperwork and evidence of actual misuse. Even then, a new
13 Social Security number may not be effective, as “[t]he credit bureaus and banks are
14 able to link the new number very quickly to the old number, so all of that old bad
15 information is quickly inherited into the new Social Security number.”⁶
16
17

18 71. This data, as one would expect, demands a much higher price on the
19 black market. Martin Walter, senior director at cybersecurity firm RedSeal,
20 explained, “[c]ompared to credit card information, personally identifiable
21 information and Social Security Numbers are worth more than 10x on the black
22
23
24
25

26 ⁶ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR,
27 Feb. 9, 2015, [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-
28 has-millions-worrying-about-identity-theft](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft) (last visited Oct. 28, 2020).

1 market.”⁷

2 72. At all relevant times, Defendant knew or reasonably should have
3 known these risks, the importance of safeguarding Private Information, and the
4 foreseeable consequences if its data security systems were breached and
5 strengthened their data systems accordingly. Defendant was put on notice of the
6 substantial and foreseeable risk of harm from a data breach, yet they failed to
7 properly prepare for that risk.
8
9

10 ***Plaintiff’s and Class Members’ Damages***

11
12 73. To date, Defendant has done little to provide Plaintiff and Class
13 Members with relief for the damages they have suffered as a result of the Cyber-
14 Attack and Data Breach, including, but not limited to, the costs and loss of time
15 they incurred because of the Cyber-Attack. Defendant has only offered 12 months
16 of inadequate identity monitoring services, and it is unclear whether that credit
17 monitoring was only offered to certain affected individuals (based upon the type of
18 data stolen) or to all persons whose data was compromised in the Cyber-Attack.
19
20

21 74. Moreover, the 12 months of credit monitoring offered to persons
22 whose private information was compromised is wholly inadequate as it fails to
23 provide for the fact that victims of data breaches and other unauthorized disclosures
24

25
26 ⁷ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
27 *Numbers*, IT World, Feb. 6, 2015, [http://www.itworld.com/article/2880960/anthem-hack-
28 personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last visited Oct.
28, 2020).

1 commonly face multiple years of ongoing identity theft and financial fraud.

2 75. Defendant entirely failed to provide any compensation for the
3 unauthorized release and disclosure of Plaintiff's and Class Members' PII.
4

5 76. Plaintiff and Class Members have been damaged by the compromise
6 of their Private Information in the Cyber-Attack.
7

8 ***Plaintiff's Experience***

9 77. Plaintiff Easley provided his PII to UTM as a condition of his
10 employment with UTM.
11

12 78. On or about February 11, 2022, Plaintiff received a Notice of Security
13 Incident Letter from UTM informing him that his full name, address and social
14 security number were stolen by cyberthieves in the Data Breach.
15

16 79. As a result of the Data Breach, UTM directed Plaintiff to take certain
17 steps to protect his PII and otherwise mitigate his damages.
18

19 80. As a result of the Data Breach and the information that he received in
20 the Notice Letter, Plaintiff spends approximately 2-3 hours per week dealing with
21 the consequences of the Data Breach (self-monitoring his bank and credit accounts),
22 as well as his time spent verifying the legitimacy of the *Notice of Data Breach*,
23 communicating with his bank, and exploring credit monitoring and identity theft
24 insurance options. This time has been lost forever and cannot be recaptured.
25

26 81. In addition, in the wake of the Data Breach, Plaintiff has had difficulty
27
28

1 with the IRS verifying his identity and filing his federal tax return for the Year 2021.
2 He has been informed his tax return is under review by the IRS. Plaintiff believes
3 these issues may be linked to the Data Breach since he has never had these issues
4 before.
5

6 82. Plaintiff is very careful about sharing his own PII and has never
7 knowingly transmitted unencrypted PII over the internet or any other unsecured
8 source.
9

10 83. Plaintiff stores any and all documents containing PII in a secure
11 location, and destroys any documents he receives in the mail that contain any PII or
12 that may contain any information that could otherwise be used to compromise his
13 identity and financial accounts. Moreover, he diligently chooses unique usernames
14 and passwords for his various online accounts.
15
16

17 84. Plaintiff suffered actual injury and damages due to Defendant's
18 mismanagement of his PII before the Data Breach.
19

20 85. Plaintiff suffered actual injury in the form of damages and diminution
21 in the value of his PII—a form of intangible property that he entrusted to Defendant
22 for the purpose of providing him payroll and benefit services, which was
23 compromised in and as a result of the Data Breach.
24

25 86. Plaintiff suffered lost time, annoyance, interference, and
26 inconvenience as a result of the Data Breach, and he has suffered anxiety and
27
28

1 increased concerns for the theft of his privacy since he received the Notice Letter.
2 He is especially concerned about the theft of his full name paired with his Social
3 Security number.
4

5 87. Plaintiff has suffered imminent and impending injury arising from the
6 substantially increased risk of fraud, identity theft, and misuse resulting from his
7 stolen PII, especially his Social Security number, being placed in the hands of
8 unauthorized third-parties and possibly criminals.
9

10 88. Plaintiff has a continuing interest in ensuring that his PII, which, upon
11 information and belief, remains backed up in Defendant's possession, is protected
12 and safeguarded from future breaches.
13

14 **CLASS ACTION ALLEGATIONS**
15

16 89. Plaintiff incorporates by reference all other paragraphs of this
17 Complaint as if fully set forth herein.
18

19 90. Plaintiff brings this action individually and on behalf of all other
20 persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure
21 23.
22

23 91. Plaintiffs propose the following Class definition(s), subject to
24 amendment based on information obtained through discovery. Notwithstanding, at
25 this time, Plaintiff brings this action and seeks certification of the following Class:
26
27
28

1 All persons whose Private Information was compromised as a result of the
2 Cyber-Attack that UTM discovered on or about May 20, 2021, and who were sent
3 notice of the Data Breach (the “Class”).
4

5 Excluded from the Class are members of the judiciary to whom this case is
6 assigned, their families and members of their staff.
7

8 92. Plaintiff reserves the right to amend the definitions of the Class or add
9 a Class if further information and discovery indicate that the definitions of the Class
10 should be narrowed, expanded, or otherwise modified.
11

12 93. Certification of Plaintiff’s claims for class-wide treatment is
13 appropriate because Plaintiff can prove the elements of their claims on a class-wide
14 basis using the same evidence as would be used to prove those elements in
15 individual actions alleging the same claims.
16

17 94. Numerosity. The Members of the Class are so numerous that joinder
18 of all of them is impracticable. While the exact number of Class Members is
19 unknown to Plaintiff at this time, based on information and belief, the Class consists
20 of 28,703 of Defendant’s current and former employees whose data was
21 compromised in the Cyber-Attack and Data Breach.
22

23 95. Commonality. There are questions of law and fact common to the
24 Class, which predominate over any questions affecting only individual Class
25 Members. These common questions of law and fact include, without limitation:
26
27
28

- 1 a) Whether Defendant unlawfully used, maintained, lost, or disclosed
2 Plaintiffs' and Class Members' Private Information;
- 3
4 b) Whether Defendant failed to implement and maintain reasonable
5 security procedures and practices appropriate to the nature and
6 scope of the information compromised in the Cyber-Attack;
- 7
8 c) Whether Defendant's data security systems prior to and during the
9 Cyber-Attack complied with applicable data security laws and
10 regulations;
- 11
12 d) Whether Defendant's data security systems prior to and during the
13 Cyber-Attack were consistent with industry standards;
- 14
15 e) Whether Defendant owed a duty to Class Members to safeguard
16 their Private Information;
- 17
18 f) Whether Defendant breached their duty to Class Members to
19 safeguard their Private Information;
- 20
21 g) Whether computer hackers obtained Class Members' Private
22 Information in the Cyber-Attack;
- 23
24 h) Whether Defendant knew or should have known that its data
25 security systems and monitoring processes were deficient;
- 26
27 i) Whether Plaintiff and Class Members suffered legally cognizable
28 damages as a result of Defendant's misconduct;

1 j) Whether Defendant's conduct was negligent;

2 k) Whether Defendant breach an implied contract between it and the
3 Plaintiffs;
4

5 l) Whether Plaintiff and Class Members are entitled to damages, civil
6 penalties, and/or injunctive relief.
7

8 96. Typicality. Plaintiff's claims are typical of those of other Class
9 Members because Plaintiff's information, like that of every other Class Member,
10 was compromised in the Cyber-Attack.
11

12 97. Adequacy of Representation. Plaintiff will fairly and adequately
13 represent and protect the interests of the members of the Class and has no interests
14 antagonistic to those of other Class Members. Plaintiff's Counsel are competent and
15 experienced in litigating data breach class actions.
16
17

18 98. Predominance. Defendant has engaged in a common course of conduct
19 toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members'
20 data was stored on the same computer systems and unlawfully accessed in the same
21 way. The common issues arising from Defendant's conduct affecting Class
22 Members set out above predominate over any individualized issues. Adjudication
23 of these common issues in a single action has important and desirable advantages
24 of judicial economy.
25
26

27 99. Superiority. A class action is superior to other available methods for
28

1 the fair and efficient adjudication of the controversy. Class treatment of common
2 questions of law and fact is superior to multiple individual actions or piecemeal
3 litigation. Absent a class action, most Class Members would likely find that the cost
4 of litigating their individual claim is prohibitively high and would therefore have
5 no effective remedy. The prosecution of separate actions by individual Class
6 Members would create a risk of inconsistent or varying adjudications with respect
7 to individual Class Members, which would establish incompatible standards of
8 conduct for Defendant. In contrast, the conduct of this action as a class action
9 presents far fewer management difficulties, conserves judicial resources and the
10 parties' resources, and protects the rights of each Class Member.
11
12
13

14 100. Defendant has acted on grounds that apply generally to the Class as a
15 whole, so that class certification, injunctive relief, and corresponding declaratory
16 relief are appropriate on a class-wide basis.
17

18 **CAUSES OF ACTION**

19 **COUNT I**

20 **NEGLIGENCE**

21 **(On Behalf of Plaintiff and All Class Members)**

22 101. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through
23 98 above as if fully set forth herein.
24

25 102. Defendant required Plaintiff and Class Members to submit non-public
26 personal information as a condition of employment or to participate in the Plans.
27
28

1 103. By collecting and storing this data in its computer property, Defendant
2 had a duty of care to use reasonable means to secure and safeguard its computer
3 property—and Class Members’ Private Information held within it—to prevent
4 disclosure of the information, and to safeguard the information from theft.
5 Defendant’s duty included a responsibility to implement processes by which they
6 could detect a breach of its security systems in a reasonably expeditious period of
7 time and to give prompt notice to those affected in the case of a data breach.
8

9
10 104. Defendant owed a duty of care to Plaintiff and Class Members to
11 provide data security consistent with industry standards and other requirements
12 discussed herein, and to ensure that its systems and networks, and the personnel
13 responsible for them, adequately protected the Private Information.
14

15
16 105. Defendant’s duty of care to use reasonable security measures arose
17 because Defendant was able to ensure that its systems were sufficient to protect
18 against the foreseeable risk of harm to Class Members from a data breach.
19

20 106. In addition, Defendant had a duty to employ reasonable security
21 measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45,
22 which prohibits “unfair . . . practices in or affecting commerce,” including, as
23 interpreted and enforced by the FTC, the unfair practice of failing to use reasonable
24 measures to protect confidential data.
25

26 107. Defendant breached its duties, and thus was negligent, by failing to use
27
28

1 reasonable measures to protect Class Members' Private Information. The specific
2 negligent acts and omissions committed by Defendant include, but are not limited
3 to, the following:
4

- 5 a. Failing to adopt, implement, and maintain adequate security
6 measures to safeguard Class Members' Private Information;
- 7 b. Failing to adequately monitor the security of their networks and
8 systems;
- 9 c. Failure to periodically ensure that their network system had plans
10 in place to maintain reasonable data security safeguards;
- 11 d. Allowing unauthorized access to Class Members' Private
12 Information;
- 13 e. Failing to detect in a timely manner that Class Members' Private
14 Information had been compromised;
- 15 f. Failing to timely notify Class Members about the Cyber-Attack so
16 that they could take appropriate steps to mitigate the potential for
17 identity theft and other damages; and
- 18 g. Failing to have mitigation and back-up plans in place in the event
19 of a cyber-attack and data breach.
20
21
22
23
24

25 108. It was foreseeable that Defendant's failure to use reasonable measures
26 to protect Class Members' Private Information would result in injury to Class
27
28

1 Members. Further, the breach of security was reasonably foreseeable given the
2 known high frequency of cyberattacks and data breaches in the financial services
3 industry.
4

5 109. It was therefore foreseeable that the failure to adequately safeguard
6 Class Members' Private Information would result in one or more types of injuries
7 to Class Members.
8

9 110. Plaintiff and Class Members are entitled to compensatory and
10 consequential damages suffered as a result of the Cyber-Attack and data breach.
11

12 111. Plaintiff and Class Members are also entitled to injunctive relief
13 requiring Defendant to (i) strengthen their data security systems and monitoring
14 procedures; (ii) submit to future annual audits of those systems and monitoring
15 procedures; and (iii) continue to provide adequate credit monitoring to all Class
16 Members.
17

18 COUNT II

19 **Negligence *Per Se*** 20 **(On Behalf of Plaintiff and All Class Members)**

21
22 112. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through
23 98 above as if fully set forth herein.

24
25 113. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C.
26 § 45, Defendant had a duty to provide fair and adequate computer systems and data
27 security practices to safeguard Plaintiffs' and Class Members' Private Information.
28

1 114. Plaintiff and Class Members are within the class of persons that the
2 FTCA was intended to protect.

3
4 115. The harm that occurred as a result of the Data Breach is the type of
5 harm the FTCA was intended to guard against. The FTC has pursued enforcement
6 actions against businesses, which, as a result of their failure to employ reasonable
7 data security measures and avoid unfair and deceptive practices, caused the same
8 harm as that suffered by Plaintiff and the Class.

9
10 116. Defendant breached its duties to Plaintiff and Class Members under
11 the Federal Trade Commission Act by failing to provide fair, reasonable, or
12 adequate computer systems and data security practices to safeguard Plaintiffs' and
13 Class Members' Private Information.

14
15 117. Defendant's failure to comply with applicable laws and regulations
16 constitutes negligence *per se*.

17
18 118. But for Defendant's wrongful and negligent breach of its duties owed
19 to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been
20 injured.

21
22 119. The injury and harm suffered by Plaintiffs and Class Members was the
23 reasonably foreseeable result of Defendant's breach of its duties. Defendant knew
24 or should have known that it was failing to meet their duties, and that Defendant's
25 breach would cause Plaintiffs and Class Members to experience the foreseeable
26
27
28

1 harms associated with the exposure of their Private Information.

2 120. As a direct and proximate result of Defendant's negligent conduct,
3
4 Plaintiffs and Class Members have suffered injury and are entitled to compensatory,
5 consequential, and punitive damages in an amount to be proven at trial.

6 **COUNT III**

7
8 **BREACH OF IMPLIED CONTRACT**
9 **(On Behalf of Plaintiff and All Class Members)**

10 121. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through
11 98 above as if fully set forth herein.

12 122. Defendant required Plaintiff and the Class to provide their personal
13 information, including name, address, and Social Security number, as a condition
14 of their employment.
15

16 123. As a condition of their employment with Defendant, Plaintiff and the
17 Class provided their personal and financial information. In so doing, Plaintiff and
18 the Class entered into implied contracts with Defendant by which Defendant agreed
19 to safeguard and protect such information, to keep such information secure and
20 confidential, and to timely and accurately notify Plaintiff and the Class if their data
21 had been breached and compromised or stolen.
22
23

24 124. Plaintiff and the Class fully performed their obligations under the
25 implied contracts with Defendant.
26

27 125. Defendant breached the implied contracts it made with Plaintiff and
28

1 the Class by failing to safeguard and protect their personal and financial
2 information, including the personal information of their beneficiaries and
3 dependents, and by failing to provide timely and accurate notice to them that
4 personal and financial information, along with the personal information of their
5 beneficiaries and dependents, was compromised as a result of the data breach.
6

7
8 126. As a direct and proximate result of Defendant's above-described
9 breach of implied contract, Plaintiff and the Class have suffered (and will continue
10 to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud,
11 and abuse, resulting in monetary loss and economic harm; actual identity theft
12 crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the
13 confidentiality of the stolen confidential data; the illegal sale of the compromised
14 data on the dark web; expenses and/or time spent on credit monitoring and identity
15 theft insurance; time spent scrutinizing bank statements, credit card statements, and
16 credit reports; expenses and/or time spent initiating fraud alerts, decreased credit
17 scores and ratings; lost work time; and other economic and non-economic harm.
18
19
20

21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiff prays for judgment as follows:
23

- 24 a) For an Order certifying this action as a class action and appointing
25 Plaintiff and his counsel to represent the Class;
26
27
28

- 1 b) For equitable relief enjoining Defendant from engaging in the
2 wrongful conduct complained of herein pertaining to the misuse
3 and/or disclosure of Plaintiffs' and Class Members' Private
4 Information, and from refusing to issue prompt, complete and
5 accurate disclosures to Plaintiff and Class Members;
6
7
8 c) For equitable relief compelling Defendant to utilize appropriate
9 methods and policies with respect to consumer data collection,
10 storage, and safety, and to disclose with specificity the type of PII
11 compromised during the Data Breach;
12
13 d) For equitable relief requiring restitution and disgorgement of the
14 revenues wrongfully retained as a result of Defendant's wrongful
15 conduct;
16
17 e) Ordering Defendant to pay for not less than five (5) years of credit
18 monitoring services for Plaintiffs and the Class;
19
20 f) For an award of actual damages, compensatory damages, nominal
21 damages, statutory damages, and statutory penalties, in an amount
22 to be determined, as allowable by law;
23
24 g) For an award of attorneys' fees and costs, and any other expense,
25 including expert witness fees;
26
27 h) Pre- and post-judgment interest on any amounts awarded; and
28

1 i) Such other and further relief as this court may deem just and proper.

2 **DEMAND FOR JURY TRIAL**

3
4 Plaintiffs demand a trial by jury on all triable issues.

5
6 Dated: March 17, 2022

Respectfully submitted,

7 */s/ Alex R. Straus*

8 Alex R. Straus (SBN 321366)

9 astraus@milberg.com

10 **MILBERG COLEMAN BRYSON**

11 **PHILLIPS GROSSMAN, PLLC**

12 280 S. Beverly Drive

13 Beverly Hills, CA 90212

14 T: 917-471-1894

15 F: 865-522-004

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Utility Trailer Facing Class Action Over 2021 Data Breach Affecting Current, Former Employees](#)
