IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE

ALTON BICKERSTAFF, individually and on behalf of all others similarly situated, Plaintiff, v. CTH RENTALS, LLC, Defendant.	**Case No.** **CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF** **JURY DEMAND**

Plaintiff Alton Bickerstaff ("Plaintiff") brings this Class Action Complaint against CTH Rentals, LLC ("Defendant" or "CTH"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving CTH Rentals, which upon information and belief, owns and/or operates several affiliated companies providing customers with rent-to-own portable storage barns throughout the United States.

2. CTH requires its customers to provide it with highly sensitive personally identifiable information ("PII"), including their full names, addresses, and Social Security numbers. Yet, CTH failed to reasonably secure, monitor, and maintain that PII. As a result, Plaintiff and approximately 140,330 other individuals ("Class Members") suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited approximately three months to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, concrete injury. These injuries include: (i) the present and imminent risk of harm arising from the access to and compromise of Plaintiff's and Class Members' PII; (ii) lost or diminished value of PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated

with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Member's PII; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

7. Plaintiff seeks to remedy these harms, and prevent any future data compromise on behalf of himself and all similarly situated persons whose PII was compromised and stolen as a result of the Data Breach, and who remain at risk due to inadequate data security.

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

II. PARTIES

Plaintiff Alton Bickerstaff

9. Plaintiff Alton Bickerstaff is a natural person domiciled in the State of Alabama.

10. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when Plaintiff rented a storage unit from Defendant.

11. Plaintiff received a notice of the Data Breach from Defendant dated January 10, 2022.

12. Since the Data Breach occurred, Plaintiff has experienced a noticeable increase in spam/scam calls and voicemail messages.

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

Defendant CTH Rentals, LLC

14. Defendant CTH Rentals, LLC is a single-member limited liability company organized in the State of Tennessee with its principal office located at 10473 US Highway 51 N Halls, TN 38040. Defendant CTH, LLC as a single member LLC with Charles T. Hammond, Jr. as the single member. Charles T. Hammond, Jr. is a citizen of the State of Tennessee. Accordingly, Defendant CTH Rentals, LLC is a citizen of the State of Tennessee.

III. JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is at least 140,330, many of whom have different citizenship from Defendant CTH, including the named Plaintiff here. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

16. This Court has jurisdiction over the Defendant because CTH because it is organized and headquartered in the State of Tennessee, its only member is domiciled in and a citizen of the State of Tennessee and in this judicial district, it operates in this District, CTH maintains Class Members' PII in Lauderdale, Tennessee, and the computer systems implicated in this Data Breach are likely based in this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is based in this District, maintains Plaintiff's and Class Members' PII in the District and have caused harm to Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Background

18. Upon information and belief, CTH owns and/or operates several affiliated companies providing customers with rent-to-own portable storage barns throughout the United States. Such companies include, but are not limited to, Southern Lease Management Group, LLC, Carolina Lease Management Group, LLC, and Sunrise Rentals, LLC, all of which are organized in the State of Tennessee with a registered principal office of 10473 US Highway 51 N Halls, TN 38040. Mr. Hammond is the statutory agent for each of these companies, and upon information and belief, is their owner and operator (either directly or indirectly through CTH).

19. Upon information and belief, Mr. Hammond and/or CTH also own and operate a rent to own storage company based in Alabama named Cotton State Barns.[1]

20. Upon information and belief, all of CTH's and/or Mr. Hammond's related entities store customer PII in a central location.

21. To rent a portable storage unit, CTH (and each of its affiliated entities) require customers to provide it with highly sensitive PII, including their full names, addresses, and Social Security numbers. Upon information and belief, this PII is then stored in a vulnerable central location. The PII held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

The Data Breach

22. According to a disclosure and sample notice letter provided to the Maine Attorney General, on September 10, 2021, CTH discovered that unauthorized individuals accessed CTH's network and/or computer systems and deployed malware causing the encryption of a number of network drives and backups.

[1] https://cottonstatebarns.com/our-story/ (last visited Jan. 17, 2022).

23. Defendant's investigation subsequently determined that the attacker(s) first gained access to its network and/or systems on August 11, 2021 and maintained this access until it encrypted Defendant's files on September 10, 2021, at which point Defendant finally detected the intrusion.

24. Upon information and belief, during the roughly one-month period that malicious cyber-criminals maintained access to Defendant's systems, the attackers accessed and acquired files on Defendant's server containing Plaintiff's and Class Members PII.

25. In a disclosure to the Maine Attorney General, CTH indicated that the PII of 140,330 individuals was compromised in the Data Breach.[2]

26. CTH did not begin sending written notifications to victims of the Data Breach (including Plaintiff Bickerstaff) until January 10, 2022.

Defendant Owes Plaintiff and Class Members a Duty to Reasonably Protect their PII

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

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

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

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/400467f9-fd08-408c-868d-8213184cf147.shtml (last visited Jan. 17, 2022).

30. The seriousness with which Defendant should have taken its data security is shown by the number of data breaches perpetrated over the past few years. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[3]

31. After a dip in 2020 to "only" 1,108 breach, 2021 will be record-breaking year for data breaches, once the final numbers are tallied. According to Identity Theft Resource Center (ITRC) research, the total number of data breaches through September 30, 2021 had already exceeded the total number of events in 2020 by 17%, with 1,291 breaches in 2021 compared to 1,108 breaches in 2020.[4]

CTH Should Have Taken Reasonable Steps to Prevent the Data Breach

32. In the notices sent to victims of the Data Breach, Defendant states that it is "taking measures to prevent a similar situation in the future." For example, "CTH has reset all passwords, deployed an end point monitoring solution, and began the process of upgrading its virus and malware protections." However, these are steps that should have been taken *before* the Data Breach.

33. Moreover, to prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC),

[3] 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 January 18, 2022)
[4] https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021 (last accessed January 18, 2022)

and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

34. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

a. **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

b. **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

c. **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d. **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

e. **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f. **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

g. **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[5]

35. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented the following measures, as recommended by the Microsoft Threat Protection Intelligence Team:

a. **Secure internet-facing assets**

Apply latest security updates

Use threat and vulnerability management

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

Perform regular audit; remove privileged credentials;

b. **Thoroughly investigate and remediate alerts**

Prioritize and treat commodity malware infections as potential full compromise;

c. **Include IT Pros in security discussions**

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

d. **Build credential hygiene**

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

e. **Apply principle of least-privilege**

Monitor for adversarial activities

Hunt for brute force attempts

Monitor for cleanup of Event Logs

Analyze logon events;

f. **Harden infrastructure**

Use Windows Defender Firewall

Enable tamper protection

Enable cloud-delivered protection

Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[6]

36. Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

37. The occurrence of the Data Breach indicates that Defendant failed to adequately

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

implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of roughly 140,000 individuals.

Defendant Failed to Comply with FTC Guidelines

38. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

39. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

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

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

take to meet their data security obligations.

42. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Value of Personally Identifiable Information

43. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

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

45. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The

---

[7] 17 C.F.R. § 248.201 (2013).
[8] *Id*.
[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 11, 2022).
[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 11, 2022).

Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[11]

46. It is incredibly difficult and time consuming to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

47. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

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

---

[11] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 11, 2022).

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Nov. 11, 2021).

49. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[13]

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

51. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

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

53. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

54. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will

---

[13] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 11, 2021).

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 11, 2022).

continue to incur such damages in addition to any fraudulent use of their PII.

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

56. In the breach notification letter, Defendant offers Class Members 12 or 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

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

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

Plaintiff's Experience

59. Plaintiff entrusted his PII to Defendant as a condition of renting a storage unit. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network drives.

60. Plaintiff received Defendant's Notice of Data Breach, dated January 10, 2022, shortly after that date.

61. The notice stated that Plaintiff's name, address, and Social Security number was among the information accessed or acquired during the Data Breach.

62. The notice offered Plaintiff identity monitoring services, fraud consultation, and identity theft restoration services, which underscores the severe nature of this Data Breach and the risk of harm to Plaintiff occasioned by Defendant allowing his Social Security number to be compromised by cybercriminals.

63. The notice specifically instructs Plaintiff to spend time taking steps to avoid identity theft and to protect his personal information, including instructing Plaintiff to change his passwords.

64. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of the Data Breach and self-monitoring his accounts and credit statements. He has also spent time changing passwords, as he was instructed to do in the Notice of Data Breach letter. This time has been lost forever and cannot be recaptured.

65. Plaintiff is very careful about sharing his PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. He is unaware of any other data breach that compromised the PII disclosed and likely acquired in the Data Breach.

66. Plaintiff stores any documents containing his PII in a safe and secure location or destroys such documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

67. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—forms of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

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

69. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from his PII being placed in the hands of unauthorized criminal third parties.

70. Plaintiff has a continuing interest in ensuring that his PII, which upon information and belief remains in Defendant's possession, is adequately protected and safeguarded from future breaches.

71. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required Plaintiff's PII when Plaintiff entered into the agreement to rent a storage unit. Plaintiff, however, would not have entrusted his PII to Defendant had he known that Defendant would fail to maintain reasonable data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

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

V. CLASS ALLEGATIONS

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

> **All persons CTH identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

74. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

75. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, but are reported to be at least 140,330. The identities of Class Members are ascertainable through CTH's records, Class Members' records, publication notice, self-identification, and other means.

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

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

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

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

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

e. Whether CTH owed a duty to Class Members to safeguard their PII;

f. Whether CTH breached its duty to Class Members to safeguard their PII;

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

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

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

j. Whether CTH's conduct was negligent;

k. Whether CTH's conduct was per se negligent, and;

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

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

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

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

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

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

a. Whether CTH owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

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

c. Whether CTH's failure to institute adequate protective security measures amounted to negligence;

d. Whether CTH failed to take commercially reasonable steps to safeguard consumer PII; and

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

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

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

84. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 83.

85. CTH knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

86. CTH had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

87. CTH had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Tenn. Code. §§ 47-18-2105 to 2107 (2005).

88. CTH had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Tenn. Code. § 47-18-2110 (2018).

89. CTH had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Tenn. Code. § 39-14-150(g).

90. CTH systematically failed to provide adequate security for data in its possession.

91. CTH, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within CTH's possession.

92. CTH, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

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

94. CTH's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

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

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

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

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

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

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

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

101. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 83.

102. Pursuant to Section 5 of the FTC Act and Tennessee law (as described above), CTH was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' PII.

103. Plaintiff and Class Members are within the class of persons whom Section 5 of the FTC Act and Tenn. Code. §§ 47-18-2105 to 2107 were designed to protect.

104. CTH breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

105. It was reasonably foreseeable, particularly given the growing number of data breaches, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII in compliance with applicable laws would result in an unauthorized third-party gaining access to CTH's networks, databases, and computers that stored or contained Plaintiff's and Class Members' PII.

106. Plaintiff's and Class Members' PII constitutes personal property that was stolen due to CTH's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

107. CTH's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted PII and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of CTH's conduct. Plaintiff and Class Members seek damages and other relief as a result of CTH's negligence.

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

108. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 83.

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

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

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

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

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

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

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

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

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

FOURTH CAUSE OF ACTION
Violations of the Tennessee Consumer Protection Act of 1977
Tenn. Code Ann. § 47-18-101, *et seq*.

118. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 83 above as if fully set forth herein. Plaintiff brings this claim on behalf of himself and the Class.

119. Plaintiff brings this cause of action pursuant to Federal Rule of Civil Procedure 23, which, procedurally, displaces any state procedural statutory ban on class actions under Tennessee's Consumer Protection Act ("TCPA").

120. Plaintiff and Class Members are "natural persons" and "consumers" within the meaning of Tenn. Code § 47-18-103(2).

121. CTH is engaged in "trade" or "commerce" or "consumer transactions" within the meaning of Tenn. Code § 47-18-103(9).

122. The TCPA prohibits "unfair or deceptive acts or practices affecting the conduct of any trade or commerce." Tenn. Code § 47-18-104.

123. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard PII;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard Private Information from theft;

c. continued gathering and storage of PII and other personal information after Defendant knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach, and;

d. continued gathering and storage of PII and other personal information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

124. These unfair acts and practices violated duties imposed by laws, including but not limited to the Section 5 of the Federal Trade Commission Act and Tenn. Code Ann. § 47-18-101, *et seq*.

125. The foregoing deceptive acts and practices were directed at consumers.

126. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to safety and security of PII.

127. CTH's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their decisions and/or conducting themselves regarding the services received from CTH.

128. Plaintiff and Class members are consumers who made payments to CTH for the furnishing of good or services (storage rental units) that were primarily for personal, family, or household purposes.

129. CTH engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of employment benefit services to consumers, including Plaintiff and Class Members.

130. CTH engaged in, and its acts and omissions affect, trade and commerce, or the furnishing of services in the State of Tennessee.

131. CTH's acts, practices, and omissions were done in the course of CTH's business of furnishing services in the State of Tennessee.

132. As a direct and proximate result of CTH's multiple, separate violations of the Tennessee CPA, Plaintiff and the Class Members suffered damages including, but not limited to: (i) the compromise, publication, and/or theft of their PII; (ii) lost time and out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use

of their PII; (iii) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (iv) the continued risk to their PII, which remains in CTH's possession and is subject to further unauthorized disclosures so long as CTH fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession, and; (v) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

133. Also as a direct result of CTH's violation of the Tennessee CPA, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering CTH to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

134. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from CTH's unfair, deceptive, and unlawful practices. CTH's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

135. CTH knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data security incident was high.

136. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

137. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages, three times actual damages, and reasonable attorneys' fees.

PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

xii. requiring Defendant to routinely and continually conduct internal training and

education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Respectfully submitted,

John Spragens, TN BPR No. 31445
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
T: (615) 983-8900
F: (615) 682-8533
john@spragenslaw.com

Terence R. Coates (*pro hac vice* forthcoming)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

David K. Lietz (*pro hac vice* forthcoming)
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW Suite 305
Washington, DC 20016
Tel: (202) 429-2290
dlietz@masonllp.com

Gary M. Klinger (*pro hac vice* forthcoming)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
gklinger@masonllp.com

Counsel for Plaintiff and the Class

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

ALTON BICKERSTAFF, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Marshall County (AL)
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

See attachment

DEFENDANTS

CTH Rentals, LLC

County of Residence of First Listed Defendant Lauderdale County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 USC 1332

Brief description of cause:
Negligence causing data breach of class members' personally identifiable information.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
01/25/2022

SIGNATURE OF ATTORNEY OF RECORD
s/ John Spragens

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

John Spragens
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
T: (615) 983-8900
F: (615) 682-8533
john@spragenslaw.com

Terence R. Coates
Dylan J. Gould
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

David K. Lietz
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW Suite 305
Washington, DC 20016
Tel: (202) 429-2290
dlietz@masonllp.com

Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
gklinger@masonllp.com

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Western District of Tennessee

ALTON BICKERSTAFF, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

CTH RENTALS, LLC,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* CTH RENTALS, LLC
10473 US Highway 51 N
Halls, TN 38040-6815

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: John Spragens
Spragens Law PLC
311 22nd Avenue North
Nashville, TN 37203

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

ClassAction.org
