IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

MARC AUBIE, individually and on behalf of all others similarly situated, Plaintiff, v. FORTRA, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Marc Aubie ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Fortra, LLC ("Defendant") and alleges as follows based on personal knowledge as to his own acts and on investigation conducted by counsel as to all other allegations:

PARTIES

1. Plaintiff Marc Aubie is a resident of Florida.

2. Defendant Fortra, LLC is a Delaware limited liability company with its principal place of business at 11095 Viking Drive, Suite 100, Eden Prairie, Minnesota, 55344.

JURISDICTION AND VENUE

3. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3)

there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class Members.

4. This Court has general personal jurisdiction over Defendant because Defendant is a resident of this state.

5. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is a resident of this district.

FACTUAL ALLEGATIONS

I. Background

6. Defendant is based in Eden Prairie, Minnesota and provides a variety of automation, cybersecurity, monitoring, storage, and transfer products to businesses worldwide.

7. One of Defendant's flagship products is GoAnywhere, a managed file transfer system that allows businesses "to centralize and secure file transfers with ease, streamline manual processes, and achieve compliance with data security standards."[1]

8. Defendant contracts with other businesses to provide secure file transfer services.

9. Other businesses use Defendant's secure file transfer services to transfer confidential files containing their own employees and clients' Personal Identifying Information ("PII").

[1] https://www.goanywhere.com/

10. When another business uses Defendant's secure file transfer services, they entrust Defendant with their confidential files, and Defendant willingly accepts responsibility for maintaining the confidentiality of the files.

11. As a sophisticated cybersecurity business with an acute interest in maintaining the confidentiality of the PII entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding PII in their possession.

II. The Data Breach

12. On or around February 2, 2023, Defendant sent a notification to its clients to notify them of a data breach to their network resulting in the unauthorized release of the clients' confidential files PII ("Data Breach").[2]

13. Defendant provided an update of its investigation of the Data Breach on April 17, 2023.[3]

> On January 30, 2023, we were made aware of suspicious activity within certain instances of our GoAnywhere MFTaaS solution. We quickly implemented a temporary service outage and commenced an investigation.
>
> We discovered between January 28, 2023, and January 30, 2023, an unauthorized party used a previously unknown, zero-day remote code execution (RCE) vulnerability to access certain GoAnywhere customers' systems. This vulnerability was assigned CVE-2023-0669.
>
> Our initial investigation revealed the unauthorized party used CVE-2023-0669 to create unauthorized user accounts in some

[2] https://www.chs.net/notice-of-third-party-security-incident-impacting-chspsc-affiliate-data/

[3] https://www.fortra.com/blog/summary-investigation-related-cve-2023-0669

> MFTaaS customer environments. For a subset of these customers, the unauthorized party leveraged these user accounts to download files from their hosted MFTaaS environments. We prioritized communication with each of these customers to share as much relevant information as available to their specific instance of the GoAnywhere platform.
>
> During the investigation, we discovered the unauthorized party used CVE-2023-0669 to install up to two additional tools - "Netcat" and "Errors.jsp" - in some MFTaaS customer environments between January 28, 2023 and January 31, 2023. The threat actor was not able to install both tools in every customer environment, and neither tool was consistently installed in every environment.
>
> When we identified the tools used in the attack, we communicated directly with each customer if either of these tools were discovered in their environment. We reprovisioned a clean and secure MFTaaS environment and worked with each MFTaaS customer to implement mitigation measures. While we continue to monitor our hosted environment, there is no evidence of unauthorized access to customer environments that have been mitigated and reprovisioned by our team.

14. The Data Breach affected approximately 130 of Defendant's clients,[4] which in turn affects those clients' employees, customers, and others who entrusted their PII to them, including Plaintiff and Class Members.

15. The PII compromised in the Data Breach likely differs among each of Defendant's clients depending on their usage of Defendant's secure file transfer services.

16. Defendant did not state why it was unable to prevent the Data Breach or which security feature failed.

[4] https://techcrunch.com/2023/03/24/fortra-goanywhere-clop-ransomware/

17. Defendant failed to prevent the Data Breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

III. Plaintiff's PII Was Compromised in the Data Breach

18. Plaintiff Marc Aubie received a letter from CHSPSC, LLC ("CHSPSC") notifying him of the Data Breach and that his PII was compromised.

19. CHSPSC, LLC is a professional services company that provides services to hospitals and clinics affiliated with Community Health Systems, Inc.[5]

20. The Data Breach affected individuals who received services at one of the CHSPSC Affiliates, are a family member or guarantor with respect to a patient, or are a current or former employee of CHSPSC Affiliate.

21. Plaintiff was a patient at a CHSPSC affiliated hospital and provided certain PII to the hospital as necessary to receive medical treatment.

22. The PII compromised in the Data Breach with respect to CHSPSC includes full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and social security number.

IV. Injuries to Plaintiff and Class Members

[5] https://www.chs.net/notice-of-third-party-security-incident-impacting-chspsc-affiliate-data/

23. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff and Class Members' PII, Plaintiff and Class Members have been injured.

24. Plaintiff and Class Members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud. Since receiving the breach notification letter, Plaintiff has been and remains very concerned and emotionally upset about the Data Breach. To this point, Plaintiff has spent approximately 20 hours doing the following activities in an effort to protect himself from the Data Breach and loss of his PII: (1) communicating with his bank to alert the bank the Plaintiff was a victim of the Data Breach; (2) filing a fraud alert with TransUnion and taking efforts through TransUnion to protect Plaintiff's governmental benefits; and (3) researching the Data Breach and what actions and steps to take to attempt to protect Plaintiff's assets and PII.

25. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

[6] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

26. In addition to fraudulent charges and damage to their credit, Plaintiff and Class Members will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

27. Additionally, Plaintiff and Class Members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value or use of their PII, and the loss of privacy.

V. Securing PII and Preventing Breaches

28. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

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

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

31. 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]

32. 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.

VI. The Value of PII

33. It is well known that PII, and social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

[7] 17 C.F.R. § 248.201 (2013).

[8] *Id.*

34. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[9]

35. People place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[10]

36. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[11] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[12]

---

[9] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[10] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[11] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[12] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

37. 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.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

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

---

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

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[15] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

> Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

39. What is more, it is no easy task 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.

40. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[17]

41. 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.

42. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card

---

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.

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

information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

43. 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.

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

45. 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.[19]

46. 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

---

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

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

Security numbers, and of the foreseeable consequences that would occur if their 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.

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

48. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in the PII that Defendant stored unencrypted, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

49. 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.

VII. Industry Standards for Data Security

50. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

51. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

52. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[20] and protection of PII[21] which includes basic security standards applicable to all types of businesses.

53. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security

[20] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[21] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

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

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

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

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

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

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[22]

55. Because Defendant was entrusted with PII, they had, and have, a duty to keep the PII secure.

56. Plaintiff and Class Members reasonably expect that when their PII is provided to a sophisticated business for a specific purpose, that business will safeguard their PII and use it only for that purpose.

57. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

CLASS ALLEGATIONS

58. This action is brought as a class action pursuant to Fed. R. Civ. P. 23.

59. The proposed Class is defined as follows:

> **Nationwide Class:** All persons whose PII was maintained on Defendant's servers that were compromised in the Data Breach.

60. The proposed Class excludes the following: Defendant, its affiliates, and its current and former employees, officers and directors, and the Judge assigned to this case.

61. The proposed Class definition may be modified, changed, or expanded based upon discovery and further investigation.

[22] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

62. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable, evidenced by the large number of individuals presently known to have been injured by Defendant's conduct. The proposed Class is ascertainable by records in the possession of Defendant or third parties.

63. *Commonality*: Questions of law or fact common to the proposed Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and Class Members to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect PII as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff and Class Members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class Members' PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Plaintiff and Class Members suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

j. Whether Plaintiff and Class Members are entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

64. *Typicality*: Plaintiff's claims are typical of the claims of proposed Class Members. Plaintiff and proposed Class Members were injured and suffered damages in substantially the same manner, have the same claims against Defendant relating to the same course of conduct, and are entitled to relief under the same legal theories.

65. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and have no interests antagonistic to those of the proposed Class. Plaintiff's counsel are experienced in the prosecution of complex class actions, including actions with issues, claims, and defenses similar to the present case.

66. *Predominance and superiority*: Questions of law or fact common to proposed Class Members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all members of the proposed Class is impracticable and the amount at issue for each proposed Class Member would not justify the cost of litigating individual claims. Should individual proposed Class Members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

67. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(3).

68. Defendant has acted, and refused to act, on grounds generally applicable to the proposed Class, thereby making appropriate final equitable relief with respect to the proposed Class as a whole.

69. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(2).

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(on behalf of the Class)

70. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

71. Defendant owed a duty of care to Plaintiff and Class Members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class Members would be harmed by such exposure of their PII.

72. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Defendant was entrusted with Plaintiff's and Class Members' PII, Defendant accepted and held the PII, and Defendant represented that the PII would be kept secure pursuant to their data security policies. Defendant alone could have ensured that their data security systems and practices were sufficient to prevent or minimize the data breach.

73. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

74. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

75. Defendant breached the aforementioned duties when it failed to use security practices that would protect Plaintiff's and Class Members' PII, thus resulting in unauthorized third-party access to the Plaintiff and Class Members' PII.

76. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit their processes, controls,

policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff and Class Members' PII within their possession, custody, and control.

77. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff and Class Members' PII was disseminated and made available to unauthorized third parties.

78. Defendant admitted that Plaintiff and Class Members' PII was wrongfully disclosed as a result of the breach.

79. The breach caused direct and substantial damages to Plaintiff and Class Members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

80. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff and Class Members' PII.

81. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

82. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have been put at an increased risk of credit fraud or identity theft, and Defendant have an obligation to mitigate damages by

providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and Class Members for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiff and Class Members to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and Class Members have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and Class Members to the extent their PII has been diminished in value because Plaintiff and Class Members no longer control their PII and to whom it is disseminated.

COUNT II

UNJUST ENRICHMENT
(on behalf of the Class)

83. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

84. Plaintiff and Class Members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

85. Defendant, by way of their acts and omissions, knowingly, and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff and Class Members' PII.

86. Defendant also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

87. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class Members. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and Class Members. The benefits conferred upon, received, and enjoyed by Defendant were not conferred gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

88. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

89. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and Class Members, wherein it profited from interference with Plaintiff and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

90. Accordingly, Plaintiff and the Class respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff and Class Members' PII, and compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Class Representative, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff demands trial by jury.

Dated: April 24, 2023

Respectfully submitted,

/s/ Bryan L. Bleichner

Bryan L. Bleichner (MN Bar #0326689)
Philip J. Krzeski (MN Bar #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700

Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Charles E. Schaffer *
Nicholas J. Elia *
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Jeffrey S. Goldenberg *
Todd B. Naylor *
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

Counsel for Plaintiff and Proposed Class

** Pro hac vice forthcoming*

JS 44 (Rev. 04/21)

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

MARC AUBIE, individually and on behalf of all others similarly situated.

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

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

Bryan L. Bleichner, Chestnut Cambronne, 100 Washington Ave. So., Suite 1700, Minneapolis, MN

DEFENDANTS

FORTRA, LLC,

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

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

Attorneys *(If Known)*

Gilbert S. Keteltas, Baker Hostetler LLP, 1050 Conneticut Ave., NW, Washington, DC 20036

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

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

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

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

INTELLECTUAL 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)***:
N/A

Brief description of cause:
Complaint for Negligent Data Security Measures

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 Susan R. Nelson DOCKET NUMBER 0:23-cv-00533

DATE
April 24, 2023

SIGNATURE OF ATTORNEY OF RECORD
s/ Bryan L. Bleichner

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.