E-FILED
Tuesday, 12 April, 2022 04:01:01 PM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
URBANA DIVISION

Michele L. Strode, *on behalf of herself and all others similarly situated,* Plaintiff, v. Christie Business Holdings Company, P.C., (d/b/a "Christie Clinic"), Defendant.	Case No. _____ Hon. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Michele L. Strode ("Plaintiff) brings this Class Action Complaint against Christie Business Holdings Company, P.C. ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including names, addresses, and Social Security numbers (collectively, "personally identifiable information" or "PII"), as well as health insurance and medical information (collectively, "protected health information" or "PHI").

2. According to Defendant's website, "[Defendant] is one of the largest physician-owned, multi-specialty group medical practices in Illinois. Established in 1929, [Defendant] has a

rich history of delivering quality and personalized healthcare to the East Central Illinois region." [1]

3. From July 14, 2021 to August 19, 2021, an unauthorized third party gained access to information in Defendant's possession (the "Data Breach"). [2]

4. During the approximately five-week Data Breach, the unauthorized third party accessed records that contained the PII and PHI of more than 500,000 individuals.

5. On or around January 27, 2022, Defendant confirmed the Data Breach took place from July 14, 2021 to August 19, 2021.

6. On or around March 25, 2022, approximately two months after Data Breach was confirmed, Defendant finally notified the United States Department of Health and Human Services. [3]

7. On or around March 24, 2022, approximately two months after the Data Breach was confirmed, Defendant finally began notifying Class Members of the Data Breach.

8. By obtaining, collecting, using, and deriving a benefit from the PII and PHI 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 admits that the unencrypted PII and PHI impacted during the Data Breach included names, addresses, Social Security numbers, health insurance information, and medical information.

9. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to

[1] https://www.christieclinic.com/about-us (last visited Apr. 12, 2022).
[2] https://www.christieclinic.com/news/5880/news-detail (last visited Apr. 12, 2022).
[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 12, 2022).

criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

10. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited several months to report it to government agencies and affected individuals. Upon information and belief, Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information.

11. As a result of this delayed response, Plaintiff and Class Members had no idea their PII and PHI 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. The risk will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting

to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and substantially increased risk to their PII and PHI, 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 and PHI.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI 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. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. 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

15. Plaintiff Michele L. Strode a Citizen of Tennessee residing in Weakley County, Tennessee.

16. Defendant Christie Business Holdings Company, P.C., (d/b/a "Christie Clinic"), is a corporation organized under the laws of Illinois, headquartered at 101 W. University Ave., Champaign, Illinois, with its principal place of business in Champaign, Illinois.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently

unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d). First, there is complete diversity between the parties—Plaintiff is a resident of the State of Tennessee and Defendant is a resident of the State of Illinois. Second, this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

20. The Central District of Illinois has personal jurisdiction over Defendant named in this action because Defendant and/or their parents or affiliates are headquartered in this District and Defendant conducts substantial business in Illinois and this District through its headquarters, offices, parents, and affiliates.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

22. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII and/or PHI, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

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

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

25. Defendant's privacy notice states, "Protecting the privacy of healthcare information is a responsibility we take very seriously. We understand that healthcare information is personal and the importance of keeping it confidential. We are committed to our established practices and procedures to protect the confidential nature of your healthcare information."[4]

26. In its privacy notice, Defendant admits it has a duty to "[1] maintain the privacy of [patients'] healthcare information; [2] provide [patients] with this [privacy] notice of [Defendant's] legal duties and healthcare information privacy practices; [and] [3] abide by the terms of this [privacy] notice." [5]

27. On or about March 24, 2022, Defendant notified the United States Department of Health and Human Resources, Plaintiff, and affected individuals ("Notice of Data Breach"). [6] Defendant advised that the information potentially impacted in the Data Breach, included names, addresses, Social Security numbers, health insurance information, and medical treatment information.

28. The Notice of Data Breach stated, in relevant part, the following:

> ***What happened?*** Christie Clinic recently discovered suspicious activity related to one of its business email accounts. **This event did not impact Christie Clinic's computer systems, electronic medical record, MyChristie patient portal, or**

[4] https://www.christieclinic.com/patient-privacy-policy (last visited Apr. 12, 2022).
[5] *Id*.
[6] *See* Notice of Data Breach Letter received by Plaintiff attached as Exhibit 1.

> **patient care**. The suspicious activity was occurring with respect to only a single user email account. Christie Clinic promptly launched an internal investigation to determine the nature and scope of this incident, and contacted federal law enforcement and worked with them to mitigate the impact of the unauthorized access. We also engaged a leading data forensics firm, and on January 27, 2022, Christie Clinic's investigation confirmed that there was unauthorized access to the affected email account from July 14, 2021 to August 19, 2021. The investigation indicated that the purpose of the unauthorized access was to intercept a business transaction between Christie Clinic and a third party vendor. This investigation was unable to determine to what extent email messages in the account were actually viewed or accessed by an unauthorized actor. As a result, Christie Clinic undertook a review to identify the full scope of information that could have been contained in the affected email account to determine whether protected information was potentially impacted. On March 10, 2022, Christie Clinic's review determined that the impacted account MAY have contained certain information related to you. We are notifying you of the incident as it MAY potentially affect the privacy of some of your information.
>
> ***What Information was Involved?*** Christie Clinic's analysis revealed that the types of information held by Christie Clinic and potentially in the affected email account MAY include your name and: address, Social Security number, medical information, and health insurance information.
>
> ***What are we doing [?]*** Christie Clinic takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we notified federal law enforcement, steps were taken to secure the impacted account and we immediately commenced an investigation to confirm the nature and scope of the incident. We have taken steps to implement additional safeguards for Christie Clinic and its patients. We already employ industry-leading network security solutions and perform regular and ongoing data security and training.

29. Defendant admitted in the Notice of Data Breach that unauthorized third persons accessed files that contained Plaintiff's and Class's Members' PII and PHI.

30. The unencrypted PII and PHI of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for more than 500,000 individuals.

32. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[7]

33. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office

[7] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

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

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[8]

34. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

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

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

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

[8] *Id.* at 3-4.

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

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[9]

35. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

[9] *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 Aug. 23, 2021).

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

36. Given that Defendant was storing the PII and PHI of more than 500,000 individuals—and likely much more than that--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 implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of more than 500,000 individuals, including Plaintiff and Class Members.

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

38. Defendant acquired, collected, and stored the PII and PHI of Plaintiff and Class Members.

39. By obtaining, collecting, and storing the PII and PHI 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 and PHI from disclosure.

[10] *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 Aug. 23, 2021).

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

Securing PII and PHI and Preventing Breaches

41. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a decade or more.

42. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

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

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] 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

[11] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

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

Value of Personal Identifiable Information

46. 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]

47. 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

[12] *Id*.
[13] *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 accessed Oct. 27, 2021).
[14] *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 accessed Oct. 27, 2021).
[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 27, 2021).

> 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.[16]

48. 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.

49. 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]

50. 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—Social Security number and name.

51. 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,

---

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 27, 2021).

[17] 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 accessed Oct. 27, 2021).

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

52. 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.

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

54. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

55. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

56. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[19]

57. Moreover, 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:

---

[18] 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 accessed Aug. 23, 2021).

[19] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

> [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.[20]

58. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers, 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.

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

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. To date, Defendant has offered Plaintiff and Class Members only 12 months of identity and credit monitoring services through Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services.

---

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

62. 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 and PHI of Plaintiff and Class Members.

Plaintiff Michele L. Strode's Experiences

63. Plaintiff entrusted her PII and PHI to Defendant.

64. At the time of the Data Breach (July 14, 2021 to August 19, 2021), Defendant retained Plaintiff's name, address, Social Security number, health insurance information, and medical information on its system.

65. Plaintiff receive Defendant's Notice of Data Breach (dated March 25, 2022) on or shortly after that date. The notice stated that Plaintiff Kroll's PII and PHI may have been among the information accessed or acquired during the Data Breach.

66. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, resetting automatic billing instructions tied to compromised credit card accounts, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

67. Plaintiff has been closely examining bank account statements and credit card statements out of fear of identity theft. Since being informed about the breach, Plaintiff has spent several hours attempting to avoid and mitigate the harm caused by the Data Breach.

68. Plaintiff is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

69. Plaintiff stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

70. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Kroll entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

71. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

72. Plaintiff has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

73. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

74. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All United States residents whose PII and/or PHI was accessed or acquired during the data breach event that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around March 25, 2022 (the "Nationwide Class").

75. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Illinois whose PII and/or PHI was actually or potentially accessed or acquired during the data breach event that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around March 25, 2021 (the "Illinois Class").

76. 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; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

77. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

78. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of individuals whose PII and/or PHI may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised the United States Department of Health and Human Services that the Data Breach affected more than 500,000 individuals.

79. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class

Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

80. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance.

81. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

82. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff have retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

83. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary

duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

84. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

85. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

86. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

87. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide

proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

88. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

89. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

90. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

91. Plaintiff and the Class entrusted Defendant with their PII and/or PHI.

92. Plaintiff and the Class entrusted their PII and/or PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and/or PHI for business purposes only, and/or not disclose their PII and/or PHI to unauthorized third parties.

93. Defendant has full knowledge of the sensitivity of the PII and/or PHI and the types of harm that Plaintiff and the Class could and would suffer if the PII and/or PHI were wrongfully disclosed.

94. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and/or PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

95. Defendant 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. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

96. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

97. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and/or PHI of Plaintiff and the Class.

98. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII and/or PHI, a necessary part of obtaining services from Defendant.

99. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

100. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

101. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and/or PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII and/or PHI, and the necessity for encrypting PII and/or PHI stored on Defendant's systems.

102. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

103. Plaintiff and the Class had no ability to protect their PII and/or PHI that was in, and possibly remains in, Defendant's possession.

104. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

105. Defendant had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and/or PHI by third parties.

106. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and/or PHI of Plaintiff and the Class.

107. Defendant has admitted that the PII and/or PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

108. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Class during the time the PII and/or PHI was within Defendant's possession or control.

109. Defendant improperly and inadequately safeguarded the PII and/or PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

110. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and/or PHI of Plaintiff and the Class in the face of increased risk of theft.

111. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII and/or PHI.

112. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

113. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

114. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and/or PHI of Plaintiff and the Class would not have been compromised.

115. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and/or PHI of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and/or PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and/or PHI by adopting, implementing, and maintaining appropriate security measures.

116. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and/or PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

117. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and/or PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and/or PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

118. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

119. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

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

121. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and/or PHI; (v) lost opportunity costs associated with effort expended

and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and/or PHI, which remain 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 and/or PHI of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

122. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

123. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and/or PHI, which remain 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 and/or PHI in its continued possession.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

125. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

126. Plaintiff and the Class entrusted their PII and/or PHI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

127. In their Privacy Policy, Defendant represented that they (i) implemented measures to help ensure an appropriate level of security for the PII and PHI/

128. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

129. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

130. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;

expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

131. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

132. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

133. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII and PHI.

134. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII and PHI.

135. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

137. Defendant acquired the monetary benefit and PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

138. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

139. Plaintiff and Class Members have no adequate remedy at law.

140. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) 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; (vi) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

141. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

142. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On behalf of Plaintiff and the Illinois Class)

143. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

144. Plaintiff and the Illinois Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Illinois Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

145. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

146. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Illinois Class's sensitive PII and PHI from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Illinois Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII and PHI of Plaintiff and the Illinois Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Illinois Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining

to the privacy and security of the PII and PHI of Plaintiff and the Illinois Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Illinois Class's PII and PHI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

147. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Class and defeat their reasonable expectations about the security of their PII and PHI.

148. Defendant intended that Plaintiff and the Illinois Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

149. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Class. Plaintiff and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

150. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Illinois Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

151. As a result of Defendant's wrongful conduct, Plaintiff and the Illinois Class were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

152. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Illinois Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff and the Illinois Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

153. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

VII. PRAYER FOR RELIEF

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

A. For an Order certifying the Nationwide Class and the Illinois Class, and appointing Plaintiff and her 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 and PHI 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 their 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 and PHI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI 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 their 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 respective 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 personal identifying information 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, but not limited to, actual, consequential, and nominal 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 demand that this matter be tried before a jury.

Date: April 12, 2022

Respectfully Submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100

Chicago, IL 60606
Telephone: (847) 208-4585
gklinger@milberg.com

Bryan L. Bleichner*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300 /Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and Putative Class

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

Michele L. Strode, on behalf of herself and all others similarly situated

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Gary M. Klinger Tel: (866) 252-0878
Milberg, Coleman, Bryson, Phillips, Grossman, PLLC
227 W. Monroe Street, Suite 2100, Chicago, IL 60606

DEFENDANTS

Christie Business Holdings Company, P.C. (d/b/a "Christie Clinic")

County of Residence of First Listed Defendant Champaign County, IL
(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

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

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

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)***:
Class Action Fairness Act 28 U.S.C. § 1332(d)

Brief description of cause:
Data Breach

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
April 12, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ Gary M. Klinger

FOR OFFICE USE ONLY

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

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

UNITED STATES DISTRICT COURT

for the

Central District of Illinois

Michele L. Strode, on behalf of herself and all others similarly situated *Plaintiff(s)* v. Christie Business Holdings Company, P.C., (d/b/a "Christie Clinic"), *Defendant(s)*	)	Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Christie Business Holdings Company, P.C.,
(d/b/a "Christie Clinic")
101 W. University Avenue
Champaign, IL 61820

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:

Gary M. Klinger,
Milberg, Coleman, Bryson, Phillips, Grossman, PLLC
227 W. Monroe Street, Suite 2100,
Chicago, IL 60606

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:

ClassAction.org