IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

HAILEY JOWERS on behalf of herself and all others similarly situated, **Plaintiff,** **v.** **CONNEXIN SOFTWARE, INC. & RALEIGH GROUP P.C., individually,** **Defendants.**	**Case No.: 5:23-CV-413** **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff, Hailey Jowers ("Plaintiff"), individually and on behalf of all others similarly situated ("Plaintiff Class Members") (and together "Plaintiffs), brings this Class Action Complaint against Connexin Software, Inc. ("Connexin"), and Raleigh Group P.C. ("Raleigh"), on behalf of itself and all others similarly situated ("Practice Group Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] and protected health information ("PHI") of more than 2.2 million current and former pediatric patients, including Plaintiffs, with the data at issue including, (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).

2. The negligence and carelessness by Defendants in maintaining the confidential data provided to them by Plaintiffs for use in their medical care could lead to severe consequences for Plaintiffs, consequences that could and should have been avoided had the Defendants taken the necessary data safety precautions.

3. Connexin provides electronic medical records and practice management software, billing services, and business analytic tools to pediatric physician practice groups, including the Practice Group Class Members.

4. Prior to and through September 13, 2022, Connexin obtained the PII and PHI of Plaintiffs from approximately 119 pediatrics physician practice groups, including Practice Group Class Members, and stored that PII and PHI, unencrypted, in an Internet-accessible environment on Connexin's network without the proper data safety precautions.

5. On or around August 26, 2022, Connexin learned of a data breach on its network that occurred on or around August 26, 2022 (the "Data Breach").

6. Connexin determined that, during this Data Breach, an unauthorized actor was able to access their systems and removed a set of data contained in an offline set of patient data used for data conversion and troubleshooting, which may have included Plaintiffs' PII and PHI.

7. At the time of the Data Breach, more than ten (10) years had passed since some Plaintiffs had obtained services from Practice Group Class Members, yet Connexin still stored their unencrypted PII and PHI on its network.

8. On or around December 6, 2022, Connexin began notifying various State Attorneys General of the Data Breach.

9. On or around December 6, 2022, Connexin began notifying Plaintiffs of the Data Breach.

10. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiffs, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII and PHI that may have been accessed and/or acquired by an unauthorized actor included (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).

11. The exposed PII and PHI of Plaintiffs can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security number, and (ii) the sharing and detrimental use of their sensitive information.

12. The PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs. In addition to Defendants' failure to prevent the Data Breach, Defendants waited more than three months after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs of that information.

13. As a result of this delayed response, Plaintiffs 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, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

14. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiffs; (ii) warn Plaintiffs of Defendants' 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. Defendants' conduct amounts to negligence and violates federal and state statutes.

15. Plaintiffs have suffered injury as a result of Defendants' 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 cost associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse as a result of Defendants' conduct; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

16. Defendants disregarded the rights of Plaintiffs by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiffs 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 Plaintiffs was compromised through disclosure to an unauthorized third party. Plaintiffs 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

17. Plaintiff Jowers is a citizen of Tennessee residing in Shelby County, Tennessee.

18. Connexin is a Maryland corporation with a principal place of business in Fort Washington, Pennsylvania.

19. Raleigh is a Tennessee corporation with its principal place of business in Memphis, Tennessee.

20. 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 Plaintiffs. Plaintiffs 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.

21. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

22. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because 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, including Plaintiff, is a citizen of a state different from Defendants to establish minimal diversity.

23. Connexin is a citizen of Maryland and Pennsylvania because it is a corporation formed under Maryland law and its principal place of business is in Fort Washington, Pennsylvania.

24. Raleigh is a citizen of Tennessee because it is a corporation formed under Tennessee law and its principal place of business is in Memphis, Tennessee.

25. The Eastern District of Pennsylvania has personal jurisdiction over Defendants because Connexin's principal place of business is found in this District and Raleigh and other Practice Group Class Members entrusted Plaintiffs' PII and PHI to Connexin in this District.

26. Venue is proper in this District under 28 U.S.C. §1391(b) because Connexin has its principal place of business in in this District, Raleigh and other Practice Group Class Members

entrusted Plaintiffs' PII and PHI to Connexin in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Background

27. Connexin collected the PII and PHI of Plaintiffs from pediatric physician practice groups, including Practice Group Class Members.

28. Plaintiffs relied on these sophisticated Defendants 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. Plaintiffs demand security to safeguard their PII and PHI.

29. Defendants had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiffs from involuntary disclosure to third parties.

B. The Data Breach

30. In December 2022, Connexin sent Plaintiffs a *Notice of Data Breach* and posted a substantially similar notice on its website (the "Website Notice"). Connexin informed Plaintiffs that:

- Connexin Software, Inc. (Connexin), a provider of electronic medical records and practice management software, billing services, and business analytic tools to pediatric physician practice groups, is providing notice that an unauthorized third party was able to gain access to an internal computer network. The live electronic medical record was not accessed and the incident did not affect any pediatric practice groups' systems, databases, or medical records system at all.
- On August 26, 2022, Connexin detected a data anomaly on our internal network. We immediately launched an investigation and engaged third-party forensic experts to determine the nature and scope of the incident. On September 13, 2022, we learned that an unauthorized party was able to access an offline set of patient data used for data conversion and troubleshooting. Some of that data was removed by the unauthorized party. The live electronic record system was not accessed in this incident, and the incident did not involve any physician practice group's systems, databases, or medical records system at all. Connexin is not aware of any actual or attempted misuse of personal information as a result of this event.
- The patient information may have included: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health

> insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all data fields may have been involved for all individuals. Information of a parent, guardian, or guarantor may also have been impacted by the incident.[2]

31. Connexin admitted in the *Notice of Data Breach* that an unauthorized actor accessed sensitive information about Plaintiffs, including (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).

32. In response to the Data Breach, Connexin claims that "[a]s soon as we discovered the incident, we immediately took action to stop the unauthorized activity. This included a password reset of all corporate accounts and moving all patient data used for data conversion and troubleshooting into an environment with even greater security. Connexin also retained a third-party cybersecurity forensic firm to investigate the issue and is working with law enforcement to investigate the incident. In response to this incident, Connexin has enhanced its security and monitoring as well as further hardened its systems as appropriate to minimize the risk of any similar incident in the future."[3] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur

[2] **Exhibit 1** - Notice Of Data Breach. Received by Hailey M. Schlafer (Maiden Name of Plaintiff Hailey Jowers). December 29, 2022.
[3] *Id.*

again have not been shared with regulators or Plaintiffs, who retain a vested interest in ensuring that their information remains protected.

33. Plaintiff additionally received notice on behalf of her minor child dated December 29, 2022.

34. The unencrypted PII and PHI of Plaintiffs may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs. Unauthorized individuals can easily access the PII and PHI of Plaintiffs.

35. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs, causing the exposure of PII and PHI for Plaintiffs.

36. Because Defendants had a duty to protect Plaintiffs' PII and PHI, Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

37. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

38. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[4]

39. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive***

[4] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), available at https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[5]

40. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[6]

41. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) cybercriminals were targeting big companies such as Defendants, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendants, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

42. In light of the information readily available and accessible on the internet before the Data Breach, Defendants, having elected to store the unencrypted PII and PHI of Plaintiffs in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and PHI and Defendants' type of business had cause to be particularly on guard against such an attack.

43. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiffs' PII and PHI could be accessed, exfiltrated, and published as the result of a cyberattack.

---

[5] KnowBe4, 1,000+ SEC Filings Show Ransomware an On-Going Risk for Public Companies (May 5, 2020)
(emphasis added), available at https://blog.knowbe4.com/1000-sec-filings-show-ransomware-an-on-going-risk-for-publiccompanies#:~:text=More%20than%201%2C000%20SEC%20documents%20filed%20with%20the,with%20another%20700%20doing%20so%20already%20in%202020. (last visited Jan. 25, 2023).

[6] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MSISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

44. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII and PHI to protect against their publication and misuse in the event of a cyberattack.

C. Defendants Acquires, Collects, and Stores the PII and PHI of Plaintiffs.

45. Practice Group Class members acquired the PII and PHI of Plaintiffs in the course of providing pediatric medical treatment.

46. Connexin obtained the PII and PHI of Plaintiffs from Practice Group Class Members and stored it on its network.

47. By obtaining, sharing, and storing the PII and PHI of Plaintiffs, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

48. Plaintiffs have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants 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.

49. 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]

50. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants 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.

[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).

- 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 written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- 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]

51. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants 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….
- **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

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

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]

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

- **Secure internet-facing assets**
  i. Apply latest security updates
  ii. Use threat and vulnerability management
  iii. Perform regular audit; remove privileged credentials;
- **Thoroughly investigate and remediate alerts:**
  i. Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  i. Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**

[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).

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

- **Apply principle of least-privilege**
  i. Monitor for adversarial activities
  ii. Hunt for brute force attempts
  iii. Monitor for cleanup of Event Logs
  iv. Analyze logon events
- **Harden infrastructure**
  i. Use Windows Defender Firewall
  ii. Enable tamper protection
  iii. Enable cloud-delivered protection
  iv. Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

53. Given that Connexin was storing the PII and PHI and PHI of more than 2.2 million individuals, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

D. Securing PII and PHI and Preventing Breaches

54. The occurrence of the Data Breach indicates that Defendants 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 and PHI of more than 2.2 million individuals, including Plaintiffs.

55. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII and PHI of Plaintiffs. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to

[10] 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).

maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

56. Defendants' negligence in safeguarding the PII and PHI of Plaintiffs is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

57. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiffs from being compromised.

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

59. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiffs 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.

E. Value of Personal Identifiable Information

60. The PII and PHI 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

[11] 17 C.F.R. § 248.201 (2013).
[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 Jan. 26, 2022).

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]

61. 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.

62. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

63. 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.

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

65. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI 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

[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-yourpersonal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

[16] 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 Jan. 26, 2022).

> 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.[17]

66. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs as a result of a breach.

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

68. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained on Connexin'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.

69. To date, Defendants have offered Plaintiffs whose Social Security numbers were impacted only one year of identity monitoring services through Kroll. The offered service is inadequate to protect Plaintiffs from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

70. The injuries to Plaintiffs were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs.

F. Plaintiff Sayers' Experience

71. Prior to the Data Breach, Plaintiff Jowers, when she was a minor child received pediatric services from Raleigh in Memphis, Tennessee.

---

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available *at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

72. Plaintiff Jowers received Connexin's *Notice of Data Breach*, dated December 29, 2022, on or about that date. The notice stated that Plaintiff Jowers personal information, including Social Security number, may have been removed from Connexin's network by an unauthorized actor and that Plaintiff Jowers may have received services from Raleigh.

73. As a result of the Data Breach, Plaintiff Jowers' sensitive information may have been removed from Connexin's network by an unauthorized actor. The confidentiality of Plaintiff Jowers' sensitive information has been irreparably harmed. For the rest of Plaintiff Jowers's life, she will have to worry about when and how her sensitive information may be shared or used to their detriment.

74. As a result of the Data Breach notice, Plaintiff Jowers spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*. This time has been lost forever and cannot be recaptured.

75. Additionally, Plaintiff Jowers 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.

76. Plaintiff Jowers 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 various online accounts that contain her sensitive information.

77. Plaintiff Jowers 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.

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

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

V. PLAINTIFF CLASS ALLEGATIONS

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

81. The Nationwide Plaintiff Class that Plaintiff seeks to represent is defined as follows:

- All individuals whose PII and PHI was compromised in the data breach that is the subject of the Notice *of Data Breach that* Defendants sent on or around December 6, 2022 (the "Nationwide Plaintiff Class").

82. Excluded from the Nationwide Plaintiff Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have 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.

83. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

84. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Plaintiff Class are so numerous that joinder of all members is impracticable. Connexin identified numerous individuals whose PII and PHI was compromised in the Data Breach, and the Nationwide Plaintiff Class is apparently identifiable within Defendants' records. Connexin reported to the United States Department of Health and Human Services that the Data Breach impacted 2,261,365 individuals.

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

i. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiffs;

ii. Whether Defendants had duties not to disclose the PII and PHI of Plaintiffs to unauthorized third parties;

iii. Whether Defendants had duties not to use the PII and PHI of Plaintiffs for non-business purposes;

iv. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiffs;

v. When Defendants actually learned of the Data Breach;

vi. Whether Defendants adequately, promptly, and accurately informed Plaintiffs that their PII and PHI had been compromised;

vii. Whether Defendants violated the law by failing to promptly notify Plaintiffs that their PII and PHI had been compromised;

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

ix. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

x. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs;

xi. Whether Plaintiffs are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

xii. Whether Plaintiffs are entitled to restitution as a result of Defendants' wrongful conduct; and

xiii. Whether Plaintiffs are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

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

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

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

89. 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 Nationwide Plaintiff 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 Nationwide Plaintiff Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Nationwide Plaintiff Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

90. The nature of this action and the nature of laws available to Plaintiffs make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Nationwide Plaintiff 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 Plaintiffs was exposed is representative of that experienced by the Nationwide Plaintiff Class and will establish the right of each Nationwide Plaintiff 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.

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

92. Adequate notice can be given to Nationwide Plaintiff Class Members directly using information maintained in Defendants' records.

93. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII and PHI of Nationwide Plaintiff Class Members, Defendants may continue to refuse to provide proper notification to Nationwide Plaintiff Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

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

95. 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:

i. Whether Defendants owed a legal duty to Plaintiffs to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

ii. Whether Defendants breached a legal duty to Plaintiffs to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

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

iv. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs on the other, and the terms of that implied contract;

v. Whether Defendants breached the implied contract;

vi. Whether Defendants adequately and accurately informed Plaintiffs that their PII and PHI had been compromised;

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

viii. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs; and,

ix. Whether Nationwide Plaintiff Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

VI. DEFENDANT PRACTICE GROUP CLASS ALLEGATIONS

96. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated against Raleigh and all others similarly situated pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure.

97. The Practice Group Class that Plaintiffs seek to certify is defined as follows:

- All pediatric physician practice groups from which Connexin obtained the PII and PHI that was compromised in the data breach that is the subject of the *Notice of Data Breach* that Connexin on or around December 6, 2022 (the "Practice Group Class").

98. Excluded from the Practice Group Class are the following individuals and/or entities: Plaintiffs and Class Members; 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.

99. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

100. Numerosity, Fed R. Civ. P. 23(a)(1): The Practice Group Class are so numerous that joinder of all members is impracticable. Connexin has identified 119 pediatric physician practice groups from which Connexin obtained the PII and PHI that was compromised in the Data Breach, and the Practice Group Class is apparently identifiable within Defendants' records.

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

i. Whether Practice Group Class Members owe a legal duty to secure the PII and PHI of Plaintiffs;

ii. Whether Practice Group Class Members continue to breach this legal duty by failing to employ reasonable measures to secure PII and PHI, including by failing to ensure that sensitive PII and PHI is encrypted and that PII and PHI is deleted if there is no reasonable need to maintain it; and

iii. Whether Practice Group Class Members' ongoing breaches of their legal duty continue to cause Plaintiffs harm.

102. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims against Raleigh are typical of those of other Practice Group Class Members because all failed to ensure that Connexin adequately safeguarded the PII and PHI compromised as a result of the Data Breach, including by failing to ensure that Connexin encrypted sensitive PII and PHI and failing to ensure that Connexin deleted PII and PHI it no longer had a reasonable need to maintain.

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

104. Adequacy, Fed. R. Civ. P. 23(a)(4): Raleigh will fairly and adequately represent and protect the interests of the Practice Group Class Members in that it has no disabling conflicts of interest that would be antagonistic to those of the other Practice Group Class Members.

105. The nature of this action and the nature of laws available to Plaintiffs embers make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs for the wrongs alleged because Practice Group Class Members would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Nationwide Plaintiff 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 Plaintiffs were exposed is representative of that experienced by the Nationwide Plaintiff 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.

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

107. Adequate notice can be given to Practice Group Class Members directly using information maintained in Defendants' records.

108. Unless a Class-wide injunction is issued, Practice Group Class Members may continue in their failure to properly secure the PII and PHI of Class Members and Practice Group Class Members may continue to act unlawfully as set forth in this Complaint.

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

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

110. Plaintiff and the Nationwide Plaintiff Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 88.

111. Connexin has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Plaintiff Class could and would suffer if the PII and PHI were wrongfully disclosed.

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

113. Connexin 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

Connexin's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Plaintiff Class in Connexin's possession was adequately secured and protected.

114. Connexin also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII and PHI it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

115. Connexin also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Plaintiff Class.

116. Connexin's duty to use reasonable security measures arose as a result of the special relationship that existed between Connexin and Plaintiff and the Nationwide Plaintiff Class. That special relationship arose because Connexin acquired Plaintiffs' and the Nationwide Plaintiff Class's confidential PII and PHI in the course of proving software services to pediatric physician practice groups from which Plaintiffs obtained medical treatment.

117. Connexin was subject to an "independent duty," untethered to any contract between Connexin and Plaintiffs or the Nationwide Plaintiff Class.

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

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

120. Connexin's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Plaintiff Class. Connexin's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Connexin's misconduct also included its decisions not to comply with industry standards for the safekeeping

of the PII and PHI of Plaintiff and the Nationwide Plaintiff Class, including basic encryption techniques freely available to Connexin.

121. Plaintiff and the Nationwide Plaintiff Class had no ability to protect their PII and PHI that was in, and possibly remains in, Connexin's possession.

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

123. Connexin had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Plaintiff Class within Connexin'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 Nationwide Plaintiff Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

124. Connexin had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Plaintiff Class.

125. Connexin has admitted that the PII and PHI of Plaintiff and the Nationwide Plaintiff Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

127. Connexin improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Plaintiff Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

128. Connexin failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Plaintiff Class in the face of increased risk of theft.

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

130. Connexin breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII and PHI it was no longer required to retain pursuant to regulations and which Connexin had no reasonable need to maintain in an Internet-accessible environment.

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

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

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

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

of its 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to its PII and PHI, which remain in Connexin's possession and is subject to further unauthorized disclosures so long as Connexin fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Plaintiff Class; and (viii) 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 the Nationwide Plaintiff Class.

135. As a direct and proximate result of Connexin's negligence, Plaintiff and the Nationwide Plaintiff 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.

136. Additionally, as a direct and proximate result of Connexin's negligence, Plaintiff and the Nationwide Plaintiff Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Connexin's possession and is subject to further unauthorized disclosures so long as Connexin fail to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

137. As a direct and proximate result of Connexin's negligence, Plaintiff and the Nationwide Plaintiff Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
INVASION OF PRIVACY
(on behalf of the Class)

138. Plaintiff and the Nationwide Plaintiff Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 88.

139. Plaintiff and the Nationwide Plaintiff Class have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information that they provide to medical service providers.

140. Defendant invaded Plaintiffs' right to privacy by allowing the unauthorized access to their PII and PHI and by negligently maintaining the confidentiality of Plaintiffs' PII and PHI, as set forth above.

141. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII and PHI was disclosed without prior written authorization from Plaintiffs.

142. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs provided and disclosed their PII and PHI to Defendant privately with an intention that the PII and PHI would be kept confidential and protected from unauthorized disclosure. Plaintiffs were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

143. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class's PII and PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiffs suffered damages as described herein.

144. Defendant is guilty of oppression, fraud, and/or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII and PHI with a willful and conscious disregard of their right to privacy.

145. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiffs great and irreparable injury in that the PII and PHI maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs, and Defendant may freely treat Plaintiff's and the Class's PII and PHI with sub-standard and insufficient protections.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of the Class)

146. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

147. Defendant invited Plaintiffs to provide their PII and PHI to Defendant. As consideration for the benefits Defendant was to administer, Plaintiffs provided their PII and PHI to Defendant. When Plaintiffs provided their PII and PHI to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII and PHI and only use it solely to administer benefits. As part of the offer, Defendant would safeguard the PII and PHI using reasonable or industry-standard means.

148. Accordingly, Plaintiffs accepted Defendant's offer to administer benefits and provided Defendant their PII and PHI.

149. Plaintiffs fully performed their obligations under the implied contracts with Defendant. However, Defendant breached the implied contracts by failing to safeguard Plaintiff's and the Class's PII and PHI.

150. The losses and damages Plaintiffs sustained that are described herein were the direct and proximate result of Defendant's breaches of its implied contracts with them. Additionally, because Plaintiffs continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiffs are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII and PHI from unlawful exposure.

151. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and it is liable to Plaintiffs for associated damages and specific performance.

COUNT IV

BREACH OF FIDUCIARY DUTY
(on behalf of the Class)

152. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

153. As alleged above, Plaintiffs had agreements with Defendant, both express and implied, that required Defendant to keep their PII and PHI confidential.

154. The parties had a fiduciary relationship of trust and confidence such that Plaintiffs relied and depended on Defendant to securely maintain their highly sensitive PII and PHI, and Defendant had a duty of care to safeguard Plaintiffs' PII and PHI.

155. Defendant breached that confidence by disclosing Plaintiff's and the Class's PII and PHI without their authorization and for unnecessary purposes.

156. As a result of the data breach, Plaintiffs suffered damages that were attributable to Defendant's failure to maintain confidence in their PII and PHI.

COUNT V
UNJUST ENRICHMENT
(on behalf of the Class)

157. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

158. Plaintiffs have an interest, both equitable and legal, in their PII and PHI that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

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

160. Defendant also understood and appreciated that the PII and PHI pertaining to Plaintiffs was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

161. 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 and PHI—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiffs. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

162. Plaintiffs, 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's and the Class's PII and PHI, Plaintiffs 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 and PHI, loss of privacy, and increased risk of harm.

163. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiffs, wherein it profited from interference with Plaintiff's and the Class's 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.

164. Accordingly, Plaintiff, on behalf of herself and the Class, respectfully requests 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's and the Class's PII and PHI, and/or compensatory damages.

COUNT VI
BAILMENT
(on behalf of the Class)

165. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

166. Plaintiffs provided, or authorized disclosure of, their PII and PHI to Defendant.

167. In allowing their PII and PHI to be made available to Defendant, Plaintiffs intended and understood that Defendant would adequately safeguard their PII and PHI.

168. For its own benefit, Defendant accepted possession of Plaintiff's and the Class's PII and PHI.

169. By accepting possession of Plaintiff's and the Class's PII and PHI, Defendant understood that Plaintiffs expected Defendant to adequately safeguard their PII and PHI. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiffs to exercise reasonable care, diligence, and prudence in protecting their personal information.

170. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and the Class's personal information, resulting in the unlawful and unauthorized access to and misuse of their PII and PHI.

171. As a direct and proximate result of Defendant's breach of its duty, Plaintiff and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

172. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiffs entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

COUNT VII
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 P.S. 201-1 *et seq.*
(on behalf of the Class)

173. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

174. Defendant is a "person" as defined by 73 P.S. § 201-2(2).

175. Plaintiff and Class members purchased goods and services in "trade" and "commerce" as defined by 73 P.S. § 201-2(3).

176. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 P.S. § 201-3, including the following:

- Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));
- Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201- 2(4)(vii)); and
- Advertising its goods and services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)).
- Defendant's unfair or deceptive acts and practices include:
    i. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Personal Information, which was a direct and proximate cause of the Breach;
    ii. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;
    iii. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
    iv. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' Personal Information, including by implementing and maintaining reasonable security measures;

v. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

vi. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Personal Information; and

vii. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

177. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

178. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

179. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs.

180. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

181. Plaintiffs acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

182. Defendant acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Class members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

183. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs' reliance on them, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

184. Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT VIII
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Plaintiff Class and Against Defendants and the Practice Group Class)

185. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 88.

186. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

187. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' PII and PHI and whether Connexin is currently maintaining data security measures adequate to protect Plaintiffs from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendants' and Practice Group Class Members' data security measures remain inadequate. Defendants and Practice Group Class Members publicly deny these allegations.

Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and PHI will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

188. Plaintiffs have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' and Practice Group Class Members' failure to encrypt Plaintiffs' and Class Members' PII and PHI, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendants' and Practice Group Class Members' failure to delete PII and PHI they had no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiffs.

189. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

i. Defendants and Practice Group Class Members owe a legal duty to secure the PII and PHI of Plaintiffs;

ii. Defendants and Practice Group Class Members continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI; and

iii. Defendants' and Practice Group Class Members' ongoing breaches of their legal duty continue to cause Plaintiffs harm.

190. This Court also should issue corresponding prospective injunctive relief requiring Defendants and Practice Group Class Members to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII and PHI. Specifically, this injunction should, among other things, direct Defendants and Practice Group Class Members to:

i. engage third party auditors, consistent with industry standards, to test Connexin's systems for weakness and upgrade any such weakness found;

ii. audit, test, and train Connexin's data security personnel regarding any new or modified procedures and how to respond to a data breach;

iii. regularly test Connexin's systems for security vulnerabilities, consistent with industry standards;

iv. implement an education and training program for appropriate employees regarding cybersecurity; and

v. ensure that Connexin encrypts sensitive PII and PHI and deletes PII and PHI it no longer has a reasonable need to maintain.

191. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Connexin. The risk of another such breach is real, immediate, and substantial. If another breach at Connexin occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

192. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants and Practice Group Class Members if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants and Practice Group Class Members of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants and Practice Group Class Members have a pre-existing legal obligation to employ such measures.

193. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Connexin, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Nationwide Plaintiff Class Members, request judgment against Defendants and the Practice Group Class and that the Court grant the following:

i. For an Order certifying the Nationwide Plaintiff Class the Practice Group Class appointing Plaintiffs and their Counsel to represent the Nationwide Plaintiff Class, and appointing Raleigh and its counsel to represent the Practice Group Class.

ii. For equitable relief enjoining Defendants and Practice Group Class Members from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiffs, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs;

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

1. prohibiting Defendants and Practice Group Class Members from engaging in the wrongful and unlawful acts described herein;
2. requiring Defendants and Practice Group Class Members to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
3. requiring Defendants and Practice Group Class Members to delete, destroy, and purge the personal identifying information of Plaintiffs unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs;
4. requiring Connexin to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs;

5. prohibiting Connexin from maintaining the PII and PHI of Plaintiffs on a cloud-based database unless sensitive PII and PHI is encrypted;
6. requiring Connexin 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 Connexin's systems on a periodic basis, and ordering Connexin to promptly correct any problems or issues detected by such third-party security auditors;
7. requiring Connexin to engage independent third-party security auditors and internal personnel to run automated security monitoring;
8. requiring Connexin to audit, test, and train its security personnel regarding any new or modified procedures;
9. requiring Connexin to segment data by, among other things, creating firewalls and access controls so that if one area of Connexin's network is compromised, hackers cannot gain access to other portions of Connexin's systems;
10. requiring Connexin to conduct regular database scanning and securing checks;
11. requiring Connexin 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 Plaintiffs;
12. requiring Connexin 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;

13. requiring Connexin 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 employee's compliance with Connexin's policies, programs, and systems for protecting personal identifying information;
14. requiring Connexin to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Connexin's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
15. requiring Connexin 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;
16. requiring Connexin to implement logging and monitoring programs sufficient to track traffic to and from Connexin'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 Connexin'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;

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

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

vi. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: February 1, 2023

Respectfully submitted,

/s/ Charles E. Schaffer
Charles E. Schaffer
Levin Sedran & Berman, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
cschaffer@lfsblaw.com

William M. Audet*
waudet@audetlaw.com
Ling (David) Y. Kuang*
lkuang@audetlaw.com
Kurt D. Kessler*
kkessler@audetlaw.com
AUDET & PARTNERS, LLP
711 Van Ness Ave., Suite 500
San Francisco, CA 94102
*(*pro hac vice forthcoming)*

Counsel for Plaintiffs

ClassAction.org