IN THE UNITED STATES DISTRICT COURT
FOT THE EASTERN DISTRICT OF PENNSYLVANIA

KAZANDRA BARLETTI, individually, as natural parent and next friend of A.B. and C.B., minors; ANDREW RECCHILONGO; SHARONDA LIVINGSTON, individually, as natural parent and next friend of K.J., a minor; BRADLEY HAIN, individually, as natural parent and next friend of N.H. and T.H., minors; HAILEY JOWERS; and IKRAM CHOWDHURY, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

CONNEXIN SOFTWARE, INC. d/b/a OFFICE PRACTICUM,

Defendant.

Case No. 2:22-cv-04676-JDW

CLASS ACTION

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Jonathan Shub
Benjamin F. Johns
Samantha E. Holbrook
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
West Conshohocken, PA 19428
(610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Bart D. Cohen
BAILEY & GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com

Interim Co-Lead Class Counsel

[*Additional Counsel on Signature Page*]

TABLE OF CONTENTS

Plaintiffs Kazandra Barletti, individually, as natural parent and next friend of A.B. and C.B., minors; Andrew Recchilongo; Sharonda Livingston, individually, as natural parent and next friend of K.J., a minor; Bradley Hain, individually, as natural parent and next friend of N.H. and T.H., minors; Hailey Jowers; and Ikram Chowdhury (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint") on behalf of themselves and all others similarly situated against Defendant Connexin Software, Inc. d/b/a Office Practicum ("Defendant" or "Connexin"). Plaintiffs make the following allegations based upon information and belief and the investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge.

NATURE OF THE CASE

1. Healthcare providers and vendors in the healthcare industry that are entrusted with patients' sensitive personally identifying information ("PII") or protected health information ("PHI") owe a duty of care to those individuals to protect that information. This duty arises because it is foreseeable that the exposure of PII and PHI (collectively "Private Information") to unauthorized persons—especially hackers and other cybercriminals with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health information. It is also foreseeable that entities entrusted with this type of sensitive data are targets for an attack. As Connexin itself acknowledges, "[c]ybersecurity breaches and ransomware attacks are becoming more common among [electronic health record] vendors."[1]

2. The harm resulting from a data breach or disclosure manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII or PHI through a data

[1] *See Protect Your Pediatric Practice and Your Data*, OFFICE PRACTICUM, https://www.officepracticum.com/office-practicum-protects-your-data-securely (last visited Apr. 27, 2023).

breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. This risk is amplified where, as here, the breached population is comprised largely of minors. As Connexin recognizes, "[p]rotecting the privacy of the very young is especially important."[2] Mitigating this ongoing threat—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take additional prophylactic measures.

3. According to the Federal Trade Commission (FTC), a child's name, address, birthday, and Social Security number can be used to commit at least the following types of fraud and identity theft:

a. Applying for government benefits, such as health care coverage or nutrition assistance;

b. Opening bank or credit card accounts;

c. Applying for loans;

d. Signing up for utility service, such as water or electricity; and

e. Renting living space.[3]

4. As a vendor providing electronic health record ("EHR") and cloud-based storage services to pediatricians, Connexin knowingly obtains sensitive patient PII and PHI and has a resulting duty to securely maintain that information in confidence.

---

[2] *See*, *Privacy Policy and Terms of Use*, OFFICE PRACTICUM, https://www.officepracticum.com/privacy-policy (last visited Apr. 27, 2023) ("Connexin's Privacy Policy").

[3] *See*, *How to Protect Your Child From Identity Theft*, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/how-protect-your-child-identity-theft (last visited Apr. 27, 2023).

5. Connexin's Privacy Policy states that it has "adopt[ed] appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information. . . and data stored" on its network.[4] Connexin's website also prominently states that "we ensure your data is secure"[5] and assures its pediatric practices that "[y]ou can place a high degree of trust behind the accuracy and integrity of the information you are storing and accessing with OP Cloud [which] exceeds best practices and industry standards for data security and preservation."[6] Connexin knows these statements are material because it recognizes that a pediatric practices' "most important business asset" is its "practice data."[7]

6. Connexin failed to uphold those promises, and failed to maintain adequate measures to protect this sensitive Private Information, which resulted in a massive data breach impacting approximately 2.2 million persons—including patients of Connexin's customers, their parents, guardians, and guarantors, as well as their insurance policyholders and payors—which Connexin purportedly discovered on August 26, 2022 (the "Data Breach").

7. Based on Connexin's own public statements about the Data Breach, a wide variety of Private Information was implicated in the breach, including but not limited to the following:

a. patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth);

b. Social Security Numbers ("SSNs");

---

[4] *See* Connexin's Privacy, s*upra* note 2.

[5] *See* Maximize Security, OFFICE PRACTICUM, https://www.officepracticum.com/who-uses/it-staff (last visited Apr. 27, 2023)

[6] *See OP Cloud Solution*, OFFICE PRACTICUM, https://www.officepracticum.com/why-choose-op/security (last visited Apr. 27, 2023)

[7] *Id.*

c. health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number);

d. medical and/or treatment information (dates of service, location, services requested, or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and

e. billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).[8]

8. As a direct and proximate result of Connexin's inadequate data security measures and breach of its duty to manage Private Information with reasonable care, Plaintiffs' and class members' Private Information has been accessed by hackers, and exposed to an untold number of unauthorized individuals, potentially on the dark web. As discussed in more detail below, certain Plaintiffs have already experienced fraud and identity theft in the aftermath of the Connexin data breach. The consequences of Connexin's misconduct and violations of law have had and will continue to have serious consequences for large numbers of young people across the nation.

9. Plaintiffs and class members are now at a significantly increased and certainly impending risk of fraud, identity theft, medical identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs and class members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiffs bring this class action on behalf of themselves and the approximately 2.2 million patients, parents, guardians, and guarantors whose PII and/or PHI was compromised in the Data Breach.

[8] *Id.*

11. On behalf of themselves and the Class as defined herein, they bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidence, breach of express contract, breach of implied contract, breach of contracts to which Plaintiffs and the Class were intended third party beneficiaries, and, in the alternative to their contract-based claims, unjust enrichment. The remedies Plaintiffs seek include actual, nominal, and putative damages; appropriate injunctive and declaratory relief; and attorneys' fees, costs, and expenses.

12. Plaintiffs seek to hold Connexin accountable for the Data Breach, including by requiring that it (i) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Connexin, (ii) provide, at its own expense, all impacted victims with identity theft protection services for an appropriate time period, and (iii) pay monetary damages.

PARTIES

Plaintiffs

13. Plaintiff Kazandra Barletti ("Plaintiff Barletti") is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Barletti resides in Croydon, Pennsylvania, and is suing on behalf of her minor son and daughter, both of whom are current patients at We Care Pediatrics, a pediatrician practice located in Langhorne, Pennsylvania. Plaintiff Barletti received a letter stating that her son's, her daughter's, and her own Private Information was compromised in the Data Breach. Upon information and belief, Plaintiff Barletti's and her son's and daughter's Private Information was provided to and received by Connexin directly or indirectly by virtue of their receiving health and health-related services from We Care Pediatrics.

14. Plaintiff Andrew Recchilongo ("Plaintiff Recchilongo") is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Recchilongo is a former patient of Drexel Hill

Pediatric Associates in Springfield, Pennsylvania. Plaintiff Recchilongo received a letter informing him that his Private Information was compromised in the Data Breach. Upon information and belief, his Private Information was provided to and received by Connexin directly or indirectly by virtue of his receiving health and health-related services from Drexel Hill Pediatric Associates.

15. Plaintiff Bradley Hain ("Plaintiff Hain") is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Hain resides in Wyomissing, Pennsylvania, and is suing on behalf of himself and his children, N.H and T.H., who were former patients at Reading Pediatrics, a pediatrician practice located in Wyomissing, Pennsylvania. Plaintiff Hain received three separate letters—one addressed to him, one addressed to his son who was a former patient of Reading Pediatrics, and one addressed to his daughter who was a former patient at Reading Pediatrics—informing him that his children's, as well as his own, Private Information was compromised in the Data Breach. Upon information and belief, Plaintiff Hain's and his children's Private Information was provided to and received by Connexin directly or indirectly by virtue of their receiving health and health-related services from Reading Pediatrics.

16. Plaintiff Sharonda Livingston ("Plaintiff Livingston") is a resident and citizen of the State of Tennessee. Plaintiff Livingston resides in Memphis, Tennessee, and is suing on behalf of her minor son, K.J., who was a patient at Raleigh Group, a pediatrician practice located in Memphis, Tennessee. Plaintiff Livingston received a letter informing her that her son's, as well as her own, Private Information was compromised in the Data Breach. Upon information and belief, Plaintiff Livingston's and her son's Private Information was provided to and received by Connexin directly or indirectly by virtue of their receiving health and health-related services from Raleigh Group.

17. Plaintiff Hailey Jowers ("Plaintiff Jowers") is a resident and citizen of the State of Tennessee. Plaintiff Jowers is a former patient of Raleigh Group. Plaintiff Jowers received a letter informing her that her Private Information was compromised in the Data Breach. Upon information and belief, her Private Information was provided to and received by Connexin directly or indirectly by virtue of her receiving health and health-related services from Raleigh Group.

18. Plaintiff Ikram Chowdhury ("Plaintiff Chowdhury") is a resident and citizen of the State of Texas. Plaintiff Chowdhury is a former patient of Pediatric Healthcare Associates of McKinney. Plaintiff Chowdhury received a letter informing him that his Private Information was compromised in the Data Breach. Upon information and belief, his Private Information was provided to and received by Connexin directly or indirectly by virtue of his receiving health and health-related services from Pediatric Healthcare Associates of McKinney.

Connexin

19. Defendant Connexin Software, Inc. is a Delaware corporation with its principal place of business located at 602 W. Office Center Drive, Suite 350, Fort Washington, Pennsylvania, 19034. Connexin refers to itself as "[t]he industry leader in pediatric-specific Health Information Technology Solutions" and claims that it "provides pediatric-specific health information technology solutions for independent pediatric practices."[9] Due to the nature of these services, Connexin acquires and electronically stores patient Private Information.

[9] *See* Office Practicum, LINKEDIN, https://www.linkedin.com/company/officepracticum/about/ (last accessed Apr. 27, 2023).

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Connexin, there are more than 100 class members, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

21. This Court has personal jurisdiction over Connexin because Connexin maintains its principal place of business in Pennsylvania and conducts substantial business in this District through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Connexin resides in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

FACTUAL BACKGROUND

A. Connexin's Promises to Safeguard Sensitive Pediatric Data

23. Founded in 1992, Connexin provides various services to its pediatrician practice clients. The company claims to have been "designed and built by pediatricians" and to understand the "challenges you face running a pediatric practice."[10]

24. Connexin describes itself as the leading provider of electronic medical records and practice management systems for use in pediatric clinical settings. It claims that its branded Office Practicum product "has provided innovative solutions to hundreds of medical practices in

[10] *See Designed for Pediatricians, by Pediatricians*, OFFICE PRACTICUM, https://www.officepracticum.com/why-choose-op/pediatric-focused (last visited Apr. 27, 2023).

over 40 states and throughout the Caribbean, ranging from solo providers to hospital-based clinics."[11]

25. Connexin sells three primary types of services to independent practices across the country: billing software, practice management software, and EHR systems.

26. EHRs are patient medical records created and used by healthcare providers.

27. Connexin claims that its proprietary EHR platform provides the "most comprehensive features for pediatric practices, including pediatric-specific decision support, screening tools and questionnaires, and vaccine management."[12]

28. Connexin offers 200 pediatric-specific well and sick visit electronic templates that can be used by physicians to memorialize patient meetings.[13] They can also be used to keep track of patient records such as immunizations and vaccines.[14]

29. A key feature offered by Connexin in connection with its EHR platform is "OP Cloud," which is a hosting service on which Connexin stores patient data remotely. Connexin first introduced it as follows in a May 23, 2012, press release:

> OP Cloud is a new hosting service provided by Connexin that provides a dynamic, virtual storage environment for its users of Office Practicum, a comprehensive EHR/EMR and Practice Management software solution designed specifically for pediatric practices and the only EHR developed by

---

[11] *Connexin Software, Inc. Receives Strategic Investment from Bluff Point Associates; Deal Will Accelerate Growth and Leadership Position of Pediatric EHR Software Provider*, BUSINESS WIRE (Nov. 16, 2011, 6:21 PM), https://www.businesswire.com/news/home/20111116006829/en/Connexin-Software-Inc.-Receives-Strategic-Investment-from-Bluff-Point-Associates-Deal-Will-Accelerate-Growth-and-Leadership-Position-of-Pediatric-EHR-Software-Provider.

[12] *See The OP Difference*, OFFICE PRACTICUM, https://www.officepracticum.com/op-difference (last visited Apr. 27, 2023).

[13] *See* Office Practicum, YOUTUBE, https://www.youtube.com/user/ConnexinSoftware (last visited Apr. 27, 2023).

[14] *Id.*

> pediatricians for pediatricians. OP Cloud will offer flexibility and efficiency for storing data in addition to instant and ensured security.
>
> With OP Cloud, all practice and patient data is stored on a protected remote server with easy accessibility through any computer or tablet with an Internet connection. The Cloud edition requires less maintenance and offers improved manageability.[15]

30. Fred Pytlak, Connexin's founder and CEO at the time, said in this press release that "[t]he OP Cloud makes it possible for providers and practice managers of pediatrician practices to increase their own productivity, as well as nurture and grow their pediatric practices, by allowing us to handle the hosting needs for OP while they concentrate on their patients and practice decision-making."[16]

31. In the regular course of its business, Connexin collects and maintains the Private Information of patients, former patients, and other persons through its provision of Office Practicum and other services to its healthcare provider customers. This sensitive information includes, *inter alia*, names, addresses, dates of birth, health insurance information, healthcare, diagnoses and treatment information, and Social Security numbers. Connexin stores this information digitally.

[15] *See Connexin Software Introduces OP Cloud*, BUSINESS WIRE (May 23, 2012, 10:00 AM), https://www.businesswire.com/news/home/20120523005105/en/Connexin-Software-Introduces-OP-Cloud.

[16] *Id.*

32. Connexin's website claims that Connexin has provided services to—and thereby, presumably, obtained sensitive Private Information of—16 million patients through the OP Cloud service it provides to healthcare providers across 40 states and throughout the Caribbean.[17] An example of one such representation appears below:

33. As noted above, Connexin acknowledges its responsibility to safeguard the highly sensitive information with which it is entrusted. For example, its marketing materials prominently assure pediatricians that security is Connexin's "top priority"[18]:

> Protecting your patient records from cyber attacks is everyone's concern. Along with the potential financial implications of a data breach, the level of trust and respect your practice has developed within your patient community is paramount to a good doctor-patient relationship.
>
> **Security is our top priority**

34. In assuring patients and providers that OP Cloud is secure, Connexin states that its data is "housed on separate systems to ensure maximum isolation from others and isolation from

[17] OFFICE PRACTICUM, https://www.officepracticum.com/ (last visited Apr. 27, 2023).

[18] *See* OP Cloud Solution, *supra*, note 6. Upon information and belief, these claims appeared on Connexin's website well before the data security incident at issue in this case.

any potential security risks."[19] The company continues: "We want you to sleep better knowing your data is safe with us."[20] The various safeguards it claims to have in place are an "added layer of security so you have peace of mind that we are looking after your most important business asset: your practice data."[21]

35. Connexin further details its security measures in at least two other documents: its Privacy Policy and its Terms of Use.

1. *Connexin's Privacy Policy*

36. Connexin's website contains the "Office Practicum Privacy Policy and Terms of Use" ("Privacy Policy") which became effective on October 1, 2018, and which were revised on February 7, 2020.[22]

37. The Privacy Policy broadly applies to the manners in which Connexin "collects, uses, maintains and discloses information collected from users," including both on the company website and in connection with "all products and services available through Office Practicum portals, website, forums, or other web- or cloud-based sites or services offered by Office Practicum."

38. The Privacy Policy states that Connexin obtains personal data in a variety of ways, including when people "visit, access, register, fill out a form, or otherwise use OP Services."[23] It delineates a limited number of ways in which Connexin may share this data, such as with "its third-party OP Service providers (such as its hosting partners) to provide the necessary hardware,

---

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *See* Connexin's Privacy Policy, s*upra,* note 2.

[23] *Id.*

software, networking, storage," or as otherwise necessary in legal proceedings or "situations involving potential threats to the physical safety of any person."[24]

39. The Privacy Policy promises that Connexin adopts "appropriate data collection, storage and processing practices and security *measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on OP Services*."[25] It underscores the foregoing by stating that Connexin does not "sell, trade, or rent" personal "identification information" to third parties.[26]

40. As noted above, Connexin recognizes in its Privacy Policy that "[p]rotecting the privacy of the very young is especially important."[27]

41. Connexin's Privacy Policy "encourage[s] Users to frequently check this page for any changes to stay informed about how we are helping to protect the personal information we collect."[28]

2. *Connexin's Terms of Use*

42. Immediately below Connexin's Privacy Policy are the "Office Practicum Terms of Use" ("Terms of Use"). Like the Privacy Policy, the Terms of Use became effective on October 1, 2018, and were revised on February 7, 2020.

43. According to Connexin, the Terms of Use "CONSTITUTE A CONTRACT" with Office Practicum (i.e., Connexin) governing the "USE OF AND ACCESS TO products and

[24] *Id.*

[25] *Id.* (emphasis added).

[26] *Id.*

[27] *Id.*

[28] *Id.*

services available through the Ideas Portal, website, forums, or other web- or cloud-based sites offered by Office Practicum ("OP Service(s)")."

44. According to Connexin, one agrees to be bound by the Terms of Use "[b]y accessing or using an OP Service, or authorizing or permitting another person or entity on your behalf to access or use the OP Service."[29]

45. Section 2 of the Terms of Use is entitled "DATA PRIVACY AND SECURITY; CONFIDENTIALITY." Sub-section 2.1, entitled "Confidential Information," includes the following mutual obligations to safeguard sensitive data:

> Subject to the express permissions of these Terms, *You and Office Practicum will protect each other's Confidential Information from unauthorized use, access or disclosure* in the same manner as each protects its own Confidential Information, but with no less than reasonable care. Except as otherwise expressly permitted pursuant to these Terms, *each of us may use each other's Confidential Information solely to exercise our respective rights and perform our respective obligations under these Terms and shall disclose such Confidential Information solely to those of our respective employees, representatives and Subscribers who have a need to know such Confidential Information for such purposes and who are bound to maintain the confidentiality of, and not misuse, such Confidential Information*.[30]

B. Connexin Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm a Data Breach Would Pose to its Patients

46. Connexin knew at all relevant times that it was storing sensitive Private Information, including that of adolescents and young children, and that, as a result, its systems would be an attractive target for cybercriminals.

47. Indeed, in trying to up-sell its own cloud-based EHR software, Connexin cited the need for pediatric practices to ensure that their patients' sensitive data is protected:

---

[29] *Id.*

[30] *Id.* (emphasis added).

> Maintaining servers can be costly, time-consuming and unpredictable, especially for pediatric offices without dedicated, top tier IT support. With rising cyber security threats, practices are facing mounting pressures to invest in complicated technologies and systems that require regular maintenance to protect patient records and ensure compliance.[31]

48. By obtaining, collecting, and storing Plaintiffs' and class members' Private Information, Connexin assumed express and implied legal duties, and knew or should have known that it was responsible for protecting Plaintiffs' and class members Private Information from unauthorized disclosure.

49. Connexin also knew that a breach of its systems and the information stored on them would result in an increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

50. These risks are not theoretical. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[32]

51. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[33]

52. The healthcare sector suffered approximately 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[34]

---

[31] *See* https://www.officepracticum.com/who-uses/it-staff.

[32] *The Healthcare Industry is at Risk*, SWIVEL SECURE, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 27, 2023).

[33] *Id.*

[34] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, HEALTH IT SECURITY (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-

53. Further, a 2022 report released by IBM Security stated that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[35]

54. The harm done to children and adolescent victims of data breaches in particular is long-lasting. Theft of minors' PHI damages children for years to come in that their identity can be stolen before they even utilize their own credit.[36]

55. Children have the potential to lose their identities to cybercriminals. Through cyberattacks hackers seize the opportunity to steal children's PII and PHI. This is not only lucrative for hackers, but doing so is hard to detect and prevent. Few people are aware of the problem and the consequences can last decades – "hackers could spen[d] more than a decade preying on a child's credit before the fraud is discovered, and by that time, it is possible that repairs will be difficult to make."[37]

56. According to the "2022 Child Identity Fraud Study" authored by Javelin Strategy & Research, approximately 915,000 children in the United States were victims of identity fraud in 2021, costing an average of $1,128 for a single household and 16 hours of remediation time.[38]

337-healthcare-data-breaches-in-first-half-of-year.

[35] *Cost of a Data Breach Report 2022*, IBM SECURITY (July 2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.

[36] Maggie Hales, *Pediatric PHI Breach Inflicts Lasting Harm*, THE HIPAA E-TOOL (Dec. 20, 2022), https://thehipaaetool.com/pediatric-phi-breach-inflicts-lasting-harm/.

[37] Elise Viebeck, *Why Hackers Want Kids' Personal Information*, THE HILL (May 23, 2015), https://thehill.com/policy/cybersecurity/242865-why-hackers-want-kids-personal-information/.

[38] *See* 1.*7 Million U.S. Children Fell victim to Data Breaches, According to Javelin's 2022 Child Identity Fraud Study*, PR NEWSWIRE (Oct. 26, 2022), https://www.yahoo.com/now/1-7-million-u-children-131000110.html#:~:text=%22Children%20often%20become%20victims%20of,or%20email%20account%20taken%20over.%22.

57. The theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Without regular monitoring, a child's identity that has been stolen may not be discovered until they are preparing to apply for student loans or get their first credit card.[39] Children are less likely to have credit reports than adults in the first place, which means a cybercriminal could establish an entire credit history long before a child realizes that they have been victimized.[40]

58. Cyberattacks against the healthcare industry have been common over the past ten years with the Federal Bureau of Investigation (FBI) warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[41]

59. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[42]

---

[39] Avery Wolfe, *How Data Breaches Affect Children*, AXIOMCYBER (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/.

[40] *See* Why Hacker's Want Kids' Personal Information, *supra* note 38.

[41] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[42] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

60. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[43]

61. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Connexin's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

62. Private Information is a valuable property right.[44] The value of Private Information as a commodity is measurable.[45] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[46] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[47] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for years afterwards.

---

[43] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 27, 2023).

[44] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[45] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[46] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[47] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

63. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

64. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[48] As indicated by Jim Trainor, former second-in-command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[49] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[50]

65. Experian elaborates on the harm that can flow from a medical data breach as follows:

---

[48] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?,* HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[49] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[50] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015,* PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[51]

66. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 has been sold or posted on the [Dark] 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."[52]

67. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a

[51] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[52] United States Government Accountability Office, Report to Congressional Requesters, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007) https://www.gao.gov/new.items/d07737.pdf.

substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

68. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[53]

69. Based on the value of its patients' PII and PHI to cybercriminals and cybercriminals' propensity to target healthcare providers, Connexin certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Connexin Breached its Promises and Legal Duties to Protect the Sensitive Data of Plaintiffs and Class Members

70. Connexin claims that, on August 26, 2022, it first "detected a data anomaly" on its "internal network."[54]

71. Connexin further claims that it engaged forensics and incident response experts to investigate the Data Breach.[55]

---

[53] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.guanotronic.com/~serge/papers/isr10.pdf.

[54] *Unauthorized Access to Internal Computer Network at Connexin Software, Inc.*, OFFICE PRACTICUM, https://www.officepracticum.com/substitute-notice/ (last visited Apr. 27, 2023) (Notice of Data Security Event).

[55] *Id.*

72. The investigation thereafter confirmed that data containing Private Information may have been accessed or acquired by an unauthorized third party.[56]

73. After the investigation revealed that Private Information may have been accessed or acquired by an unauthorized third party, Connexin conducted a review process to confirm what it already knew—that Private Information of current and former patients had been compromised.[57]

74. As noted above, the patient Private Information compromised in the Data Breach includes patient names, dates of birth, Social Security numbers, financial account and payment information, medical information, and health insurance information.[58]

75. On or around the time that Connexin reported the Data Breach to the Attorneys General of Montana and Texas, Connexin provided notice to Plaintiffs indicating that their Private Information may have been compromised or accessed, approximately four months after Connexin first discovered the Data Breach.[59]

76. It appears that the Data Breach occurred entirely on Connexin's servers: "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."

77. The breach did, however, impact patient data that, at a minimum, previously had been provided by patients to their physicians who then provided it to Connexin. Connexin revealed that it was providing notice of the breach on behalf of itself and the following 119 physician practices/practice groups across the country (the "Pediatrician Practices"):

---

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] https://www.officepracticum.com/substitute-notice/

- Eastern Shore Children's Clinic, PC, located in Spanish Fort, AL
- KION Pediatrics, PLLC, located in Jonesboro, AK
- Maryvale Pediatric Specialists, LLC, located in Phoenix, AZ
- Springfield Medical, LLC, located in San Tan Valley, AZ
- Central Coast Pediatrics, Inc., located in San Luis Obispo, CA
- Jaleh Niazi, M.D., PC d/b/a New Day Pediatrics, located in Berkeley, CA
- James A. Weidman, AMC, located in West Hills, CA
- Orland Children's Center, Inc., located in Orland, CA
- San Marino Pediatric Associates, located in San Marino, CA
- Valley Children's Medical Group, located in Madera, CA
- Thompson River Pediatrics and Urgent Care, LLC, located in Johnstown, CO
- Winsted Pediatrics, located in Winsted, CT
- Angel Kids Pediatrics, located in Jacksonville, FL
- Children's Health of Ocala, PA, located in Ocala, FL
- Kidswood Pediatrics, Inc., located in Winter Park, FL
- Mariano D. Cibran, M.D., Inc. d/b/a St. Petersburg Pediatrics, in St. Petersburg, FL
- Pediatric Associates, PA, located in Pembroke Pines, FL
- Pediatric Care Center No. 2, Inc., located in West Palm Beach, FL
- Pensacola Pediatrics PA, located in Pace, FL
- Raza Ali, MD, PC, located in Orlando, FL
- Yazji Pediatrics, located in St. Johns, FL
- Children's Pediatric Center Northside, LLC, located in Canton, GA
- Graham Pediatrics of Woodstock, LLC, located in Woodstock, GA

- Kids World Pediatrics, LLC, located in Fayetteville, GA
- Pediatric Associates of Lawrenceville, LLC, located in Lawrenceville, GA
- Pediatric Center for Wellness, PC, located in Conyers, GA
- Pediatric Medicine of Cartersville, PC, located in Cartersville, GA
- Phillips Pediatrics, PC, located in Hinesville, GA
- Sumter Pediatrics, LLC, located in East Americus, GA
- Children's Mercy – Shawnee Mission Pediatrics, located in Merriam, KS
- Great Bend Children's Clinic, PA, located in Great Bend, KS
- Advanced Care Pediatric Centre, PLLC, located in Danville, KY
- Madison Pediatric Associates, PC, located in Richmond, KY
- Pediatric Associates, PSC, located in Crestview Hills, KY
- Dr. Michael J Ulich Pediatrics, LLC, located in Minden, LA
- Emily B. Vigour, M.D., LLC d/b/a Vigour Pediatrics, located in Marrero, LA
- Rachel Z. Chatters, M.D., Inc, located in Lake Charles, LA
- Alice Tanner, M.D., PC, located in Glen Burnie, MD
- Cecilia A Nwankwo, M.D. FAAP, PC, located in Gaithersburg, MD
- Discovery Pediatrics, Inc., located in Silver Spring, MD
- Forest Hill Pediatrics, LLC MD, located in Forrest Hill, MD
- Honeygo Pediatrics, LLC, located in Nottingham MD
- Jose F. Alvarado & Associates, PA, located in Salisbury, MD
- Maryland Pediatric Care, LLC, located in Germantown, MD
- Ruth Agwuna, M.D., located in Ellicott City, MD
- Samuel R Williams, M.D., PA, located in Catonsville, MD

- South River Pediatrics, LLC, located in Edgewater, MD
- The Pediatric Center of Frederick, LLC, located in Frederick, MD
- Harbor Pediatrics, PS, located in York, ME
- Fox Pediatrics, PLLC, located in Mt. Pleasant, MI
- Mayura Madani, M.D., PLLC, located in Detroit, MI
- Petoskey Pediatrics PC, located in Petoskey, MI
- Watch Us Grow Pediatrics, PC, located in Trenton, MI
- Children's Mercy – Pediatric Partners, Inc., located in Kansas City, MS
- Children's Health Center of Columbus, Inc., located in Columbus, MS
- McComb Children's Clinic, Ltd., located in McComb, MS
- Rankin Children's Group, PLLC, located in Flowood, MS
- Helena Pediatric Clinic, PC, located in Helena, MT
- Eastern Carolina Pediatrics, PA, located in Wilson, NC
- Goldsboro Pediatrics, PA, located in Goldsboro, NC
- Kidzcare Pediatrics, PC, located in Fayetteville, NC
- QC Kidz Pediatrics, PLLC, located in Charlotte, NC
- Thomasville-Archedale Pediatrics, PLLC, located in Trinity, NC
- Lilac City Pediatrics, PA, located in Rochester, NH
- Academy Pediatrics, PA, located in Manalapan, NJ
- Gaurang Patel, M.D., LLC, located in Colonia, NJ
- Hawthorne Pediatrics, LLC, located in Hawthorne, NJ
- Holmdel Pediatrics, LLC, located in Holmdel, NJ
- Jackson Pediatric Associates, PA, located in Jackson Township, NJ

- Passaic Pediatrics II, PA, located in Passaic, NJ
- Pediatric MultiCare West, LLC, located in Pompton Lakes, NJ
- SCS LLC d/b/a Bayshore Pediatrics, located in Toms River, NJ
- Fraser-Branche Medical, PLLC, located in Batavia, NY
- Heights Pediatrics, PC, located in Brooklyn, NY
- Peds First Pediatrics, located in Medford, NY
- SchoolCare, Inc. f/k/a CareDox, Inc., located in New York, NY
- Premiere Pediatrics, PLLC, located in Norman, OK
- Texoma Pediatrics, PLLC, located in Durant, OK
- Westview Pediatric Care, LLC, located in Tulsa, OK
- Oregon City Pediatrics, located in Oregon City, OR
- All Star Pediatrics, LLC, located in Exton, PA
- Drexel Hill Pediatric Associates, PC, located in Springfield, PA
- Ekta Khurana, M.D., PLLC, located in Philadelphia, PA
- Hatboro Pediatrics, PC, located in Hatboro, PA
- Kids First Pediatric Care, PA, located in Philadelphia, PA
- Kressly Pediatrics, PC, located in Warrington, PA
- Reading Pediatrics, Inc., located in Wyomissing, PA
- We Care Pediatrics, PC, located in Langhorne, PA
- Zero Pediatrics, PLLC, located Dunmore, PA
- Carolina Pediatrics and Adolescent Care, PA, located in Colombia, SC
- Kids Kare Pediatrics, PLLC, located in Philadelphia, PA
- Cordova Pediatrics, PLLC, located in Cordova, TN

- Crockett Kids Pediatrics, PC, located in Lawrenceburg, TN
- Goodlettsville Pediatrics, PC, located in Goodlettsville, TN
- Pediatrics East, PC, located in Arlington, TN
- Raleigh Group, PC, located in Memphis, TN
- Hebron Pediatrics, LLC, located in Carrollton, TX
- Arlington Pediatric Partners, PLLC d/b/a Kids Docs Pediatrics, in Arlington, TX
- August Pediatrics, PA, located in Decatur, TX
- Austex Pediatrics, PA, located in Austin, TX
- Casey Thomas Mulcihy Austin Texas, PA, located in Austin TX
- Ennis Pediatric and Adolescent Health Care, PA, located in Ennis, TX
- Gold Pediatrics, PA, located in Arlington TX
- Kerrville Pediatrics, PLLC, located in Kerrville, TX
- Maria Luisa Lira, M.D., PA, located in Corpus Christi, TX
- Northeast Pediatric Night Clinic, Inc., located in El Paso, TX
- Pediatric Health Center of El Paso, located in El Paso, TX
- Pediatric Healthcare Associates of McKinney, located in McKinney, TX
- Sistema Infantil Teleton USA, Inc. a/k/a CRITS, located in San Antonio, TX
- The Pediatric & Adolescent Clinic, Inc., located in Richardson, TX
- Wee Tots Pediatrics, PA, located in Arlington, TX
- ABC Pediatrics Practice, PC, located in Fredericksburg, VA
- Bristow Pediatrics, PLLC, located in Manassas, VA
- Children’s Clinic, Ltd., located in Newport News, VA
- Kate Bowers, M.D., PLLC d/b/a Firefly Pediatrics, located in Midlothian, VA

- Pediatric Physicians of Reston, PC, located in Reston, VA
- Renaissance Pediatrics, P.C., located in Chesapeake, VA
- Virginia Pediatric Group, Ltd., located in Fairfax, VA
- Community Pediatrics, SC, located in Beaver Dam, WI

78. Plaintiffs and class members all received materially identical notices informing them that their PII and/or PHI was exposed in the Data Breach.

79. Overall, more than 2,200,000 individuals—including patients of Connexin, their parents, guardians, and guarantors, as well as their insurance policyholders and payors— had their PII and/or PHI breached.[60]

80. The Data Breach occurred as a direct result of Connexin's failure to implement and follow basic security procedures to protect its customers' patients' (and their guardians') Private Information.

D. Plaintiffs' Experiences

1. *Plaintiff Barletti*

81. After the Data Breach, and in addition to the injuries alleged above, Plaintiff Barletti has experienced fraudulent transactions in her son's name that she believes resulted from her Private Information being compromised in the Data Breach. Specifically, in or about August or September 2022, Plaintiff Barletti discovered a late payment report on her credit report from an unknown vendor listed as "Emergency Services of PA" that purportedly provided emergency services for her son even though no such services were ever provided. Plaintiff Barletti was subsequently contacted by a collection agency, Westfield & Associates, about the overdue bill for emergency services that she never procured. Plaintiff Barletti called Westfield & Associates

[60] *Id.*

back to dispute the charge since no such services were ever provided to her son and was informed that they would be disputed. As of the date of the filing of this complaint, the fraudulent credit report of overdue payment for "Emergency Services of PA" remains on her credit report and is damaging her credit score. As a result, Plaintiff Barletti was forced to spend multiple hours disputing this fraudulent report on her credit.

82. Plaintiff Barletti has spent approximately 5 to10 hours contacting Connexin and We Care Pediatrics about the data breach, contacting and dealing with the fraudulent report on her credit for a past due bill from "Emergency Services of PA," and checking her and her children's credit and financial accounts for any unauthorized activity following the Data Breach, a practice Plaintiff Barletti is forced to continue indefinitely to protect against fraud and identity theft. The time spent on checking her financial accounts is time directly attributable to the Data Breach.

83. Plaintiff Barletti plans to take additional time-consuming, necessary steps to mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

2. *Plaintiff Recchilongo*

84. After the Data Breach, and in addition to the injuries alleged above, Plaintiff Recchilongo has experienced a significant uptick in suspicious and phone calls and text messages, including phishing attempts.

85. Plaintiff Recchilongo has spent approximately 6.5 hours checking his credit and financial accounts for any unauthorized activity following the Data Breach, a practice Plaintiff Recchilongo is forced to continue indefinitely to protect against fraud and identity theft. The time spent on checking his financial accounts is time directly attributable to the Data Breach.

86. Plaintiff Recchilongo plans to take additional time-consuming, necessary steps to mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

3. *Plaintiff Livingston*

87. After the Data Breach, and in addition to the injuries alleged above, Plaintiff Livingston has experienced fraudulent transactions that she believes resulted from her Private Information being compromised in the Data Breach. Specifically, in or about August or September 2022, an unknown, unauthorized individual opened a bank account with Wells Fargo in Plaintiff Livingston's name. As a result, Plaintiff Livingston was forced to spend multiple hours contacting all three major U.S. credit bureaus to freeze her credit.

88. Plaintiff Livingston has spent approximately 10 hours checking her credit and financial accounts for any unauthorized activity following the Data Breach, a practice Plaintiff Livingston is forced to continue indefinitely to protect against fraud and identity theft. The time spent on checking her financial accounts is time directly attributable to the Data Breach.

89. Plaintiff Livingston plans to take additional time-consuming, necessary steps to mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

4. *Plaintiff Hain*

90. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Hain has spent approximately an hour checking his financial accounts for any unauthorized activity following the Data Breach and notifying his children of the data breach and instructing them to do the same, a practice Plaintiff Hain and his children are forced to continue

indefinitely to protect against fraud and identity theft. The time spent on checking their financial accounts is time directly attributable to the Data Breach.

91. Plaintiff Hain plans to take additional time-consuming, necessary steps to mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

5. *Plaintiff Jowers*

92. After the Data Breach, and in addition to the injuries alleged above, Plaintiff Jowers also experienced actual identity theft and fraud, including unauthorized charges to her credit card and an increase in spam text messages and calls.

93. Plaintiff Jowers has spent approximately 10 to 15 hours responding to these incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time directly attributable to the Data Breach.

94. Plaintiff Jowers plans to take additional time-consuming, necessary steps to mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

6. *Plaintiff Chowdhury*

95. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Chowdhury also experienced actual identity theft and fraud as a result of his Private Information being exposed, including: having his Yahoo email account taken over and eventually deemed unrecoverable; attempted access by unauthorized third parties of his Gmail account, Steam account, and UBI Soft account; an attempted log in to his Allstate Insurance account; a

fraudulent attempt to open a Capital One Account in his name; and a significant increase in spam calls and texts.

96. Plaintiff Chowdhury has spent approximately 10 to 15 hours responding to these incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time directly attributable to the Data Breach.

97. Plaintiff Chowdhury plans to take additional time-consuming, necessary steps to mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

E. Connexin is Obligated Under HIPAA to Safeguard Personal Information

98. Connexin is required by the Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1302d, *et seq*. ("HIPAA") to safeguard patient PHI.

99. Connexin is an entity covered by HIPAA, which sets minimum federal standards for privacy and security of PHI. As a covered entity, Connexin has a statutory duty under HIPAA to safeguard Plaintiffs' and class members' PHI.

100. Connexin's website states that it "offers a secure and HIPPA [sic] compliant cloud solution that works hand-in-hand with your EHR and PM software."[61]

101. HIPAA establishes national standards for the protection of PHI. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. This includes compliance with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A

[61] *See* No Practice is too Big or too Small, OFFICE PRACTICUM, https://www.officepracticum.com/who-uses/providers-of-all-sizes (last visited Apr. 27, 2023).

and E (Standards for Privacy of Individually Identifiable Health Information"), and the Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

102. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

103. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" and (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and also either (a) "identifies the individual;" or (b) "with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

104. HIPAA requires Connexin to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

105. HIPAA also requires Connexin to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under C.F.R. § 164.306(e), and to "[i]implement technical policies and procedures for electronic information systems that maintain electronic

protected health information to allow access only to those persons or software programs that have been granted access rules." 45 C.F.R. § 164.312(a)(1).

106. Further, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also required Connexin to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[62] Connexin did not comply with that Rule.

107. While HIPAA permits covered entities to disclose PHI to third parties under certain circumstances, HIPAA does not permit them to disclose PHI to cybercriminals nor did Plaintiffs or class members consent to the disclosure of their PHI to cybercriminals.

108. As such, Connexin is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and class members' PHI that it requires, receives, and collects, and Connexin is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

109. Given the application of HIPAA to Connexin, and that Plaintiffs and class members entrusted their PHI to it to receive healthcare services, Plaintiffs and class members reasonably expected that Connexin would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit Connexin from Engaging in Unfair or Deceptive Acts or Practices

110. Connexin is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce."

[62] *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Apr. 27, 2023).

The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[63]

111. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[64]

112. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[65]

113. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[66]

---

[63] *See Prepared Statement of the Federal Trade Commission before the Committee on Homeland Security and Governmental Affairs*, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, UNITED STATES SENATE (Mar. 7, 2019), https://www.ftc.gov/system/files/documents/public_statements/1466607/commission_testimony_re_data_security_senate_03072019.pdf.

[64] *Start with Security – A Guide for Business*, U.S. FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[65] *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[66] *Id.*

114. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

115. Connexin failed to properly implement basic data security practices. Connexin's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

116. As discussed above, Connexin was fully aware of its obligations to protect the Private Information of patients because of its position as a vendor in the healthcare industry, which gave it direct access to a large volume of patient PII and PHI. Connexin was also aware of the significant repercussions that would result from its failure to do so.

G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

117. Cyberattacks and data breaches at healthcare companies like Connexin are especially problematic because they can negatively impact the daily lives of individuals affected by the attacks.

118. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[67]

[67] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

119. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes.[68]

120. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[69]

121. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

122. Theft of Private Information is serious. The FTC warns consumers that identity

[68] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RESEARCH 971, 971-980 (Sept. 10, 2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[69] *See* U.S. Gov. Accounting Office, *supra* note 53.

thieves use Private Information to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

123. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[70]

124. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

125. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

126. The privacy of Private Information is a valuable property right.[71]

---

[70] *See IdentityTheft.gov*, FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last accessed Apr. 27, 2023).

[71] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally*

127. Theft of medical data in particular is gravely serious: "The thief may use your identity to see a doctor. He or she may get prescription drugs or to file claims with your insurance company in your name. If the thief's medical treatment or diagnosis mixes with your treatment or diagnosis, your health is at risk."[72]

128. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII/PHI stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and class members.

129. Social Security numbers are particularly sensitive personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [73]

Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[72] *See First Aid for Medical Identity Theft: Tips for Consumers*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, https://oag.ca.gov/privacy/facts/medical-privacy/med-id-theft (last visited Apr. 28, 2023).

[73] *See also Dark Web Monitoring: What You Should Know*, CONSUMER FED'N OF AM. (Mar. 19, 2019) (emphasis added).

130. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[74]

131. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[75] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[76] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

132. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[77]

133. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble and risk of running a targeted cyberattack against

---

[74] *Id.*

[75] *Id.*

[76] *Id.* at 4.

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

companies like Connexin is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[78]

134. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[79] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[80]

135. The medical information which was exposed is also highly valuable. PHI can sell for as much as $363 according to the Infosec Institute.[81]

136. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they will use it.[82]

137. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum.[83] "Victims often experience financial repercussions and worse yet, they frequently

---

[78] Tim Green, *Anthem hack: Personal data stolen sells for 10X price of stolen credit card numbers*, COMPUTERWORLD (Feb. 6, 2015), https://www.computerworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[79] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PCMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[80] *Dark Web Monitoring: What You Should Know*, CONSUMER FED'N OF AM. (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[81] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Apr. 27, 2023).

[82] *Id.*

[83] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS, (Feb.

discover erroneous information has been added to their personal medical files due to the thief's activities."[84]

138. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[85] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[86] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[87] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[88]

139. A report published by the World Privacy Forum and presented at the FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.

7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[84] *Id.*

[85] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.

[86] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions, PUB. INTEL.* (May 6, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions.

[87] *What to Know About Medical Identity Theft*, FED. TRADE COMM'N (Aug. 2019), https://consumer.ftc.gov/sites/default/files/articles/pdf/973a-medical-idtheft-what-to-know-what-to-do-508_0.pdf.

[88] *Id.*

- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[89]

140. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, an individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

141. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[90]

---

[89] *FTC Informational Injury Workshop*, FED. TRADE COMM'N (October 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

[90] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 5 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

142. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [91] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[92]

143. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[93]

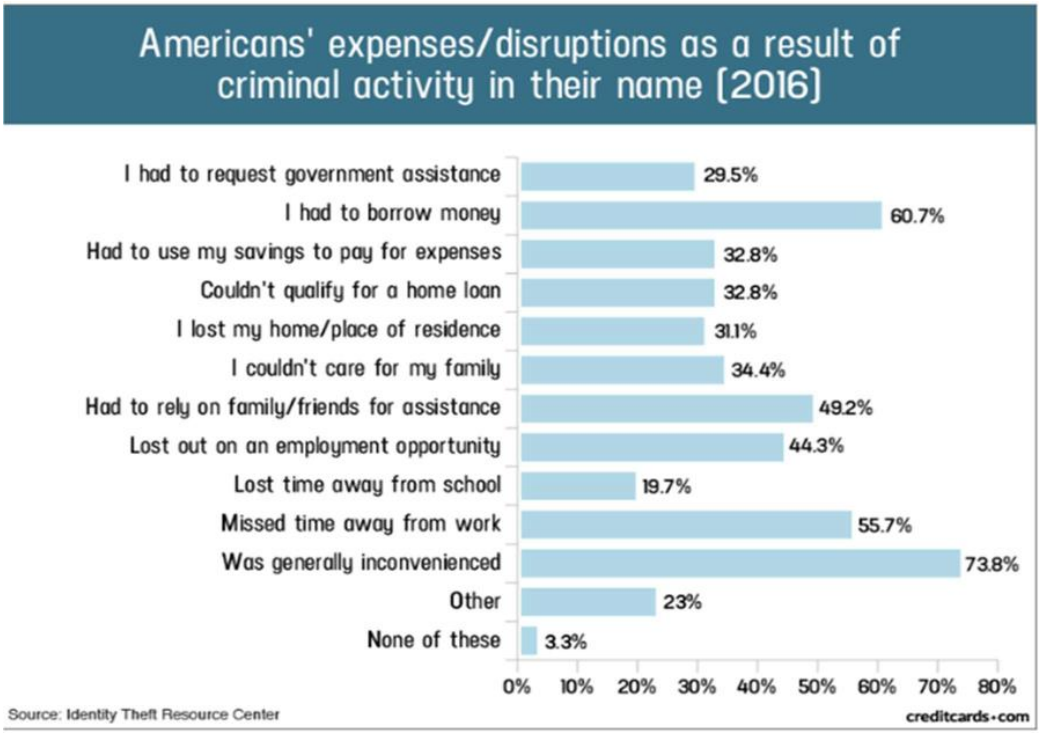
144. It is within this context that Plaintiffs and all other class members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and frauds, including making the information available for sale on the black market.

145. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

[91] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 27, 2023).

[92] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), Experian (April 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[93] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.



146. Victims of the Data Breach, like Plaintiffs and class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[94]

147. As a direct and proximate result of the Data Breach, Plaintiffs and class members have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank

[94] *Id.*

accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

148. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Connexin knew or should have known about these dangers and strengthened its data security accordingly. Connexin was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

H. Plaintiffs and Class Members Suffered Damages Because of Connexin's Misconduct

149. Connexin was provided with and otherwise received Plaintiffs' Private Information in connection with its customers' provision of certain medical services and treatment to them. In maintaining Plaintiffs' Private Information for business purposes, Connexin expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' Private Information. Connexin did not, however, take proper care of Plaintiffs' Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Connexin's inadequate security measures.

150. In or about December 2022, Connexin sent Plaintiffs a breach notice concerning the Data Breach. The notice letter states that on September 13, 2022, Connexin learned that an unauthorized party was able to access an offline set of patient data used for data conversion and troubleshooting, and that some of that data was removed by the unauthorized party. The notice letter further states that the compromised information 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, (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). The notice further encouraged Plaintiffs "to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid" and to report "any questionable charges" to the provider's billing office, or for insurance statements, to the patient's insurance company. Connexin also offered identity theft protection services through Kroll, but only for a period of one year.

151. Connexin's data security shortcomings resulted in the Data Breach and caused Plaintiffs significant injuries and harm in several ways. For example, Plaintiffs have devoted and will continue to devote significant time, energy, and money to: closely monitoring their medical statements, bills, records, and credit and financial accounts; changing login and password information on any sensitive account; carefully screening and scrutinizing phone calls, emails, and other communications to ensure that they are not being targeted by identity theft scams, medical identity theft scams, or other attempts at fraud; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect themselves; and placing fraud alerts and/or credit freezes on their credit file. Plaintiffs have taken or will be forced to take these measures to mitigate their potential damages because of the Data Breach.

152. Once PII and PHI are exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and class members will need to maintain these heightened measures for years, and possibly their entire lives because of Connexin's conduct.

153. Plaintiffs had a reasonable expectation of privacy while receiving medical services. Plaintiffs would not have agreed to have their sensitive Private Information provided to and maintained by Connexin had they known that Connexin would fail to adequately protect their Private Information. Indeed, Plaintiffs sought medical care through providers that used Connexin's services with the reasonable expectation that their medical providers' vendors, like Connexin, would keep their Private Information secure and inaccessible to unauthorized parties. Plaintiffs and class members would not have obtained services from Connexin had they known that Connexin failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII/PHI from criminal theft and misuse.

154. Further, the value of Plaintiffs' and class members' Private Information has been diminished by its exposure in the Data Breach. Plaintiffs and class members did not receive the full benefit of their bargain when paying for medical services. Plaintiffs and class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they received.

155. As a result of Connexin's failures, Plaintiffs and class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

156. Further, because Connexin delayed in notifying Plaintiffs and class members about the Data Breach for over three months, Plaintiffs were unable to take affirmative steps during that period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

157. According to one study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[95]

158. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[96] Indeed, in 2013 alone, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States," which is more than identity thefts involving banking, finance, the government and the military, or education.[97]

159. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[98] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[99]

---

[95] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Apr. 27, 2023).

[96] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTH IT SECURITY (Sept. 25, 2019) https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[97] Michael Ollove, *supra* note 83.

[98] Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[99] *Id.*; *see also* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (Mar. 31, 2023), /www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

160. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[100]

161. Plaintiffs and class members are also at a continued risk because their information remains in Connexin's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Connexin fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

CLASS ACTION ALLEGATIONS

162. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiffs seeks certification of a Nationwide Class as defined below:

> **Nationwide Class:** All persons in the United States and its territories whose Private Information was compromised in the Data Breach, including all individuals who received a data breach notification letter from Connexin.

163. In addition, or in the alternative to the Nationwide Class, Plaintiffs seek to represent each of the following state-wide classes (the Nationwide Class and State-Wide Classes are collectively referred to as the "Class"):

> **Pennsylvania Class:** All persons in Pennsylvania whose Private Information was compromised in the Data Breach, including all individuals who received a data breach notification letter from Connexin.
>
> **Texas Class:** All persons in Texas whose Private Information was compromised in the Data Breach, including all individuals who received a data breach notification letter from Connexin.

[100] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

> **Tennessee Class:** All persons in Tennessee whose Private Information was compromised in the Data Breach, including all individuals who received a data breach notification letter from Connexin.

164. Excluded from the Class are Connexin, its subsidiaries and affiliates, officers and directors, any entity in which Connexin have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

165. The proposed class definitions are based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definitions in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery proceeds.

166. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

167. Numerosity: The classes are so numerous that joinder of all class members in a single proceeding would be impracticable. According to Connexin, approximately 2.2 million individuals' information was exposed in the Data Breach.

168. Commonality and Predominance: Common questions of law and fact exist as to all class members and predominate over any potential questions affecting only individual class members. Such common questions of law or fact include, *inter alia:*

a. Whether Connexin had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and class members' Private Information from unauthorized access and disclosure;

b. Whether Connexin's actions and its allegedly lax data security practices used to protect Plaintiffs' and class members' PII and PHI violated the FTC Act, HIPAA, and/or other state laws and/or Connexin's other duties alleged herein;

c. Whether Connexin failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and class members;

d. Whether Plaintiffs and class members suffered injury as a proximate result of Connexin's negligent actions or failures to act;

e. Whether Connexin failed to exercise reasonable care to secure and safeguard Plaintiffs' and class members' Private Information;

f. Whether an implied contract existed between class members and Connexin providing that Connexin would implement and maintain reasonable security measures to protect and secure class members' Private Information from unauthorized access and disclosure;

g. Whether an express contract existed between class members and Connexin providing that Connexin would implement and maintain reasonable security measures to protect and secure class members' Private Information from unauthorized access and disclosure;

h. Whether Plaintiffs and class members are intended third party beneficiaries of contracts between Connexin and third parties, and if so whether Connexin breached those contracts;

i. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and class members;

j. Whether Connexin's actions and inactions alleged herein constitute gross negligence;

k. Whether Connexin breached its duties to protect Plaintiffs' and class members' Private Information; and

l. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

169. Connexin engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

170. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the class, had their Private Information compromised in the Data Breach. Plaintiffs and class members were injured by the same wrongful acts, practices, and omissions committed by Connexin, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all class members.

171. Adequacy: Plaintiffs will fairly and adequately protect the interests of the class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

172. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Connexin, so it would be impracticable for class members to individually seek redress from Connexin's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

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

174. Unless a class-wide injunction is issued, Connexin may continue to maintain inadequate security with respect to the Private Information of class members, Connexin may continue to refuse to provide proper and adequate notice to class members regarding the Data Breach, and Connexin may continue to act unlawfully.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

175. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

176. Plaintiffs bring this claim individually and on behalf of the Class.

177. Connexin owed a duty to Plaintiffs and class members to exercise reasonable care in safeguarding and protecting their PII and PHI in its possession, custody, and control. It also had a common law duty to prevent foreseeable harm to others.

178. Connexin's duty to use reasonable care arose from several sources, including but not limited to those described below.

179. This duty existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices on the part of the Connexin. By collecting and storing valuable Private Information that is routinely targeted by criminals for unauthorized access, Connexin was obligated to act with reasonable care to protect against these foreseeable threats.

180. Connexin's duty also arose from its position as a vendor in the healthcare industry that was entrusted with highly sensitive patient data. Both as a matter of law and based upon the various assertions made by Connexin as described above, it assumed a duty to reasonably protect its patients' information. Indeed, Connexin was in a unique and superior position to protect against the harm suffered by Plaintiffs and class members as a result of the Data Breach.

181. Connexin breached the duties it owed to Plaintiffs and class members. As a result of a successful attack directed towards Connexin that compromised Plaintiffs' and class members' Private Information, Connexin breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information

safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

182. But for Connexin's wrongful and negligent breach of its duties owed to Plaintiffs and class members, their Private Information would not have been compromised.

183. As a direct and proximate result of Connexin's negligence, Plaintiffs and class members have suffered injuries, including, but not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and

identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Connexin with the mutual understanding that Connexin would safeguard Plaintiffs' and class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Connexin's possession and is subject to further breaches so long as Connexin fails to undertake appropriate and adequate measures to protect Plaintiffs' and class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and class members.

184. As a direct and proximate result of Connexin's negligence, Plaintiffs and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Class)

185. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

186. Plaintiffs bring this claim individually and on behalf of the Class.

187. 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 entities such as Connexin for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Connexin's duty.

188. Connexin violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Connexin's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving Private Information of its customers' patients.

189. Plaintiffs and class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

190. Connexin's violation of Section 5 of the FTC Act constitutes negligence per se.

191. Connexin is an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

192. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Connexin had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiffs' and the class members' electronic PHI.

193. Specifically, HIPAA required Connexin to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of

the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

194. Connexin violated HIPAA by actively disclosing Plaintiffs' and class members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and class members' PHI.

195. Plaintiffs and the class members are patients within the class of persons HIPAA was intended to protect.

196. Connexin's violation of HIPAA constitutes negligence *per se*.

197. The harm that has occurred as a result of Connexin's conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

198. As a direct and proximate result of Connexin's negligence, Plaintiffs and class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class)

199. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

200. Plaintiffs bring this claim individually and on behalf of the Class.

201. Plaintiffs and class members have an interest, both equitable and legal, in their Private Information that was conveyed to, collected by, and maintained by Connexin and that was accessed or compromised in the Data Breach.

202. As a recipient of patients' Private Information, Connexin has a fiduciary relationship to its customers' patients, including Plaintiffs and the class members.

203. Because of that fiduciary relationship, Connexin was provided with and stored private and valuable Private Information related to Plaintiffs and the Class. Plaintiffs and class members were entitled to expect their information would remain confidential while in Connexin's possession.

204. Connexin owed a fiduciary duty under common law to Plaintiffs and class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Connexin's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

205. As a result of the parties' fiduciary relationship, Connexin had an obligation to maintain the confidentiality of the information within Plaintiffs' and class members' medical records.

206. Connexin's customers' patients, including Plaintiffs and class members, have a privacy interest in personal medical matters, and Connexin had a fiduciary duty not to disclose medical data concerning its customers' patients.

207. As a result of the parties' relationship, Connexin had possession and knowledge of confidential Private Information of Plaintiffs and class members, information not generally known.

208. Plaintiffs and class members did not consent to nor authorize Connexin to release or disclose their Private Information to unknown criminal actors.

209. Connexin breached its fiduciary duties owed to Plaintiffs and class members by, among other things:

a. mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer

information that resulted in the unauthorized access and compromise of PII and PHI;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

210. But for Connexin's wrongful breach of its fiduciary duties owed to Plaintiffs and class members, their Private Information would not have been compromised.

211. As a direct and proximate result of Connexin's breach of its fiduciary duties, Plaintiffs and class members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Connexin with the mutual understanding that Connexin would safeguard Plaintiffs' and class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Connexin's possession and is subject to further breaches so long as Connexin fails to undertake appropriate and adequate measures to protect Plaintiffs' and class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime

opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and class members.

212. As a direct and proximate result of Connexin's breach of its fiduciary duties, Plaintiffs and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Class)

213. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

214. Plaintiffs bring this claim individually and on behalf of the Class.

215. Plaintiffs and class members have an interest, both equitable and legal, in their Private Information that was conveyed to, collected by, and maintained by Connexin and that was accessed or compromised in the Data Breach.

216. Connexin was provided with and stored private and valuable PHI related to Plaintiffs and the Class, which it was required to maintain in confidence.

217. Plaintiffs and the Class provided Connexin with their personal and confidential PHI under both the express and/or implied agreement of Connexin to limit the use and disclosure of such PHI.

218. Connexin owed a duty to Plaintiffs and class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

219. Connexin had an obligation to maintain the confidentiality of Plaintiffs' and class members' PHI.

220. Plaintiffs and class members have a privacy interest in their personal medical matters, and Connexin had a duty not to disclose confidential medical information and records concerning its patients.

221. As a result of the parties' relationship, Connexin had possession and knowledge of confidential PHI and confidential medical records of Plaintiffs and class members.

222. Plaintiffs' and class members' PHI is not generally known to the public and is confidential by nature.

223. Plaintiffs and class members did not consent to nor authorize Connexin to release or disclose their PHI to unknown criminal actors.

224. Connexin breached the duties of confidence it owed to Plaintiffs and class members when Plaintiffs' and class members' PHI was disclosed to unknown criminal hackers.

225. Connexin breached its duties of confidence by failing to safeguard Plaintiffs' and class members' PHI, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and

practices published to its patients; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs and the class members' PHI and medical records/information to a criminal third party.

226. But for Connexin's wrongful breach of its duty of confidences owed to Plaintiffs and class members, their privacy, confidences, and PHI would not have been compromised.

227. As a direct and proximate result of Connexin's breach of Plaintiffs' and class members' confidences, Plaintiffs and class members have suffered injuries, including:

a. Loss of their privacy and confidentiality in their PHI;

b. Theft of their Private Information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Connexin Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

h. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Connexin with the mutual understanding that Connexin would safeguard Plaintiffs' and class members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Connexin's possession and is subject to further breaches so long as Connexin fails to undertake appropriate and adequate measures to protect Plaintiffs' and class members' data;

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Connexin; and

k. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

228. Additionally, Connexin received payments from Plaintiffs and class members for services with the understanding that Connexin would uphold its responsibilities to maintain the confidences of Plaintiffs' and class members' private medical information.

229. Connexin breached the confidence of Plaintiffs and class members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI and, accordingly, it would be inequitable for Connexin to retain the benefit at Plaintiffs' and class members' expense.

230. As a direct and proximate result of Connexin's breach of its duty of confidences, Plaintiffs and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On behalf of Plaintiffs and the Class)

231. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

232. Plaintiffs bring this claim individually and on behalf of the Class.

233. Plaintiffs and class members had a reasonable expectation of privacy in the PII/PHI Connexin mishandled.

234. Connexin's conduct as alleged above intruded upon Plaintiffs' and class members' seclusion under common law.

235. By intentionally failing to keep Plaintiffs' and class members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Connexin intentionally invaded Plaintiffs' and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and class members' private affairs in a manner that identifies Plaintiffs and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and class members.

236. Connexin knew that an ordinary person in Plaintiffs' or class members' position would consider Connexin's intentional actions highly offensive and objectionable.

237. Connexin invaded Plaintiffs' and class members' right to privacy and intruded into Plaintiffs' and class members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

238. Connexin intentionally concealed from and delayed reporting to Plaintiffs and class members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

239. The conduct described above was at or directed at Plaintiffs and class members.

240. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Connexin's conduct amounted to a substantial and serious invasion of Plaintiffs' and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Connexin's intentional actions or inaction highly offensive and objectionable.

241. In failing to protect Plaintiffs' and class members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Connexin acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and class members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

242. As a direct and proximate result of Connexin's conduct, Plaintiffs and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

243. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein. This claim is pled in the alternative to the breach of express contract claim and all the other claims herein.

244. Plaintiffs bring this claim individually and on behalf of the Class.

245. When Plaintiffs and class members provided their Private Information to Connexin, they entered into implied contracts with Connexin, under which Connexin agreed to take reasonable steps to protect Plaintiffs' and class members' Private Information, comply with it statutory and common law duties to protect Plaintiffs' and class members' Private Information, and to timely notify them in the event of a data breach.

246. Connexin solicited and invited Plaintiffs and class members to provide their Private Information as part of Connexin's provision of healthcare services. Plaintiffs and class members accepted Connexin's offers and provided their Private Information to Connexin.

247. When entering into implied contracts, Plaintiffs and class members reasonably believed and expected that Connexin's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and class members' PII and PHI and to timely notify them in the event of a data breach.

248. Connexin's implied promise to safeguard patient Private Information is evidenced by, *e.g.*, the representations in Connexin's Notice of Privacy Practices set forth above.

249. Plaintiffs and class members paid money to Connexin's customers to receive healthcare services. Plaintiffs and class members reasonably believed and expected that Connexin would use part of those funds to obtain adequate data security. Connexin failed to do so.

250. Plaintiffs and class members would not have provided their Private Information to Connexin had they known that Connexin would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

251. Plaintiffs and class members fully performed their obligations under their implied contracts with Connexin.

252. Connexin breached its implied contracts with Plaintiffs and class members by failing to safeguard Plaintiffs' and class members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

253. The losses and damages Plaintiffs sustained, include, but are not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Connexin with the mutual understanding that Connexin would safeguard Plaintiffs' and class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Connexin's possession and is subject to further breaches so long as Connexin fails to undertake appropriate and adequate measures to protect Plaintiffs' and class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and class members.

254. As a direct and proximate result of Connexin's breach of contract, Plaintiffs and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiffs and the Class)

255. Plaintiffs restate and reallege the preceding allegations the paragraphs above as if fully alleged herein. This claim is pleaded in the alternative to the breach of implied contract claim and all the other claims herein.

256. Plaintiffs bring this claim individually and on behalf of the Class.

257. Connexin's Privacy Policy created an express contractual obligation to safeguard and protect the sensitive information of Plaintiffs and class members.

258. The Privacy Policy also contractually promised that Connexin would only share Plaintiffs' and class members' Private Information to certain authorized recipients in only a limited set of circumstances.

259. Connexin breached both of these contractual duties by failing to adequately safeguard Plaintiffs' and class members' Private Information, and by allowing it to be disseminated to unauthorized third parties.

260. Plaintiffs and class members substantially performed their part of the bargain.

261. Connexin's breach of these contractual obligations in the Privacy Policy and elsewhere caused damages to Plaintiffs and class members, as set forth herein.

EIGHTH CAUSE OF ACTION
BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD PARTY BENEFICIARIES
(On behalf of Plaintiffs and the Class)

262. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein. This claim is pleaded in the alternative to the breach of implied contract claim and all the other claims herein.

263. Plaintiffs bring this claim individually and on behalf of the Class.

264. Connexin had valid contracts with each of the Pediatrician Practices. A principal purpose of those contracts was to securely store, transmit and safeguard the Private Information of Plaintiffs and class members.

265. Upon information and belief, Connexin and each of the contracting Pediatrician Practices expressed an intention that Plaintiffs and class members were intended third party beneficiaries of these agreements.

266. Plaintiffs and class members are also intended third party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Connexin intended to give the beneficiaries the benefit of the promised performance.

267. Connexin breached its agreements with the contracting Pediatrician Practices by allowing the data breach to occur, and as otherwise set forth herein.

268. Connexin's breach caused foreseeable and material damages to Plaintiffs and class members.

NINTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

269. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

270. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' contractual based claims pursuant to Fed. R. Civ. P. 8.

271. Upon information and belief, Connexin funds its data security measures utilizing payments made by or on behalf of Plaintiffs and the class members.

272. As such, a portion of the payments made by or on behalf of Plaintiffs and the class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Connexin.

273. Plaintiffs and class members conferred a monetary benefit on Connexin. Specifically, they purchased healthcare services from Connexin and/or its agents and in so doing

provided Connexin with their Private Information. In exchange, Plaintiffs and class members should have received from Connexin the goods and services that were the subject of the transaction and had their Private Information protected with adequate data security.

274. Connexin knew that Plaintiffs and class members conferred a benefit which Connexin accepted. Connexin profited from these transactions and used the Private Information of Plaintiff and class members for business purposes.

275. In particular, Connexin enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and class members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Connexin instead elected to increase its own profits at the expense of Plaintiffs and class members by utilizing cheaper, ineffective security measures. Plaintiffs and class members, on the other hand, suffered as a direct and proximate result of Connexin's decision to prioritize its own profits over the requisite security.

276. Under the principles of equity and good conscience, Connexin should not be permitted to retain the money belonging to Plaintiffs and class members, because Connexin failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

277. Connexin failed to secure Plaintiffs and class members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and class members provided.

278. Connexin acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

279. If Plaintiffs and class members knew that Connexin had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Connexin.

280. Plaintiffs and class members have no adequate remedy at law.

281. As a direct and proximate result of Connexin's conduct, Plaintiffs and class members have suffered and will continue to suffer other forms of injury and/or harm.

282. Connexin should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and class members, proceeds that it unjustly received from them. In the alternative, Connexin should be compelled to refund the amounts that Plaintiffs and class members overpaid for Connexin's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an order certifying the Class under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For monetary damages, including compensatory, nominal, and punitive damages, in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all claims so triable.

Dated: April 28, 2023

/s/ Bart D. Cohen

Bart D. Cohen
BAILEY & GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com

Jonathan Shub
Benjamin F. Johns
Samantha E. Holbrook
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
West Conshohocken, PA 19428
(610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Plaintiffs' Interim Co-Lead Counsel

Andrew Ferich
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
T: (310) 474-9111
F: (310) 474-8585
aferich@ahdootwolfson.com

Mark B. DeSanto
SAUDER SCHELKOPF LLC
1109 Lancaster Ave
Berwyn, PA 19312
mbd@sstriallawyers.com

Danielle Perry
MASON LLP
5101 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
dperry@masonllp.com

Marc Edelson
EDELSON LECHTZIN LLP
411 S. State Street, Suite N-300
Newtown, PA 18940
(215) 867-2399
medelson@edelson-law.com

Michael McShane
AUDET & PARTNERS, LLP
711 Van Ness Avenue, Ste 500
San Francisco, CA 94102
(415) 568-2555
mmcshane@audetlaw.com

Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that I caused the foregoing Consolidated Class Action Complaint to be filed on this 28th day of April 2023, thereby serving it upon counsel of record for all parties via the Court's CM/ECF system.

/s/ Bart D. Cohen
Bart D. Cohen