

**IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT,  
IN AND FOR MIAMI-DADE COUNTY, FLORIDA**

**PAUL JEFFERSON, EVELYN SANDS,  
and BRIDGETT CONNOR**, individually  
and on behalf of all others similarly situated,

Plaintiffs,

v.

**COMMUNITY CONNECTIONS, INC.,**

Defendant.

**Case No.:**

**COMPLAINT – CLASS ACTION**

**JURY TRIAL DEMANDED**

Plaintiffs Paul Jefferson, Evelyn Sands, and Bridgett Connor (collectively, “Plaintiffs”), individually and on behalf of all other similarly situated persons (the “Class” or “Class Members” (as further defined below)), allege the following against Defendant Community Connections, Inc. (“Community Connections” or “Defendant”) based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs’ counsel and review of public documents as to all other matters:

**I. INTRODUCTION**

1. Plaintiffs bring this class action against Community Connections for its failure to secure and safeguard Plaintiffs’ and the Class’s personally identifiable information (“PII”) and protected health information (“PHI”) from criminal hackers, resulting in two (2) massive and preventable data breaches.<sup>1</sup>

---

<sup>1</sup> OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications, Community Connections*, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/71000ad5-97b5-4314-ba35-fb6f5d3f6e0a.html> (last visited May 11, 2026).

2. Community Connections is a behavioral health agency based in Washington, D.C. that provides mental health and clinical housing services.<sup>2</sup>

3. Plaintiffs and the Class are current and former employees and patients of Community Connections.

4. Community Connections collected and maintained Plaintiffs' and Class Members' PII and PHI during the course of obtaining services.

5. On or about August 22, 2025, Community Connections reported to the Maine Attorney General's office that it had experienced a sizable data breach involving the PII and PHI of approximately 20,876 individuals (the "First Data Incident").<sup>3</sup> Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

6. On or about August 28, 2025, Community Connections sent out notice of data breach letters ("Notice Letters") to individuals whose PII/PHI was compromised as a result of the First Data Incident.

7. Based on the Notice Letters sent to Plaintiffs and Class Members, on October 21, 2024, Community Connections discovered unusual activity on its computer systems.<sup>4</sup> In response, Defendant alleges it engaged a cybersecurity firm to conduct an investigation to determine the nature and scope of the First Data Incident.<sup>5</sup> Community Connections' investigation revealed that an unauthorized party had access to certain files that contained the highly sensitive PII and PHI of Plaintiffs and the Class.

---

<sup>2</sup> COMMUNITY CONNECTIONS, *Our Mission*, <https://communityconnectionsdc.org/mission> (last visited May 11, 2026).

<sup>3</sup> OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications, Community Connections*, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/71000ad5-97b5-4314-ba35-fb6f5d3f6e0a.html> (last visited May 11, 2026).

<sup>4</sup> *Id.* (containing a link to a sample Notice Letter).

<sup>5</sup> *Id.*

8. However, the Notice Letters fail to mention the start date and end date of the First Data Incident. Thus, the First Data Incident could have lasted for *weeks*.

9. Despite learning of the First Data Incident in October 2024, Community Connections inexplicably waited *nearly one (1) year* to notify the victims—Plaintiffs and Class Members.

10. As a result of this delayed response, Plaintiffs and Class Members had no idea—for *approximately ten (10) months*—that their PII and PHI had been compromised, and that Plaintiffs and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will remain for their respective lifetimes.

11. According to Defendant, the types of PII and PHI compromised in the First Data Incident includes, but is not limited to: (i) full names; (ii) addresses; (iii) dates of birth; (iv) Social Security numbers; (v) financial information; (vi) driver’s license or state identification information; (vii) medical information; and (viii) health insurance information (collectively, “Private Information”). The Private Information exposed is highly sensitive, representing a gold mine for data thieves.

12. On or about April 4, 2026, Community Connections experienced *another* data breach to its computer systems by an unauthorized party (the “Second Data Incident”) (the First Data Incident and the Second Data Incident collectively referred to as the “Data Incidents”).

13. The Second Data Incident was reportedly perpetrated by notorious cybercriminal ransomware group, Inc Ransom, as pictured below: <sup>6</sup>

---

<sup>6</sup> See, e.g., HOOKPHISH (April 4, 2026), *Ransomware Group incransom Hits: Community Connections*, <https://www.hookphish.com/blog/ransomware-group-incransom-hits-community-connections/> (last visited May 11, 2026); REDPACKET SECURITY (April 4, 2026), *[INCRANSOM]*—

INC Ransom

News

Disclosures

Report

New York 11:25 pm

Los Angeles 10:25 pm

London 02:25 am

Paris 03:25 am

Moscow 04:25 am

Beijing 09:25 am

Tokyo 10:25 am

Blog / Disclosures / 69c90c9e8f1d14b743f59f93

coronapa.com

🇺🇸

74

Kentucky Injury

🇺🇸

7374

Infonet Media d.o.o.

🇷🇸

148

BERGE-BAU GmbH & Co. KG

🇩🇪

178

roodtrucking.com

🇺🇸

344

lrpea.it

🇮🇹

948

pulpdent.com

🇺🇸

3571

submissionfinance.com

🇺🇸

1849

Community Connections

🇺🇸

46

Community Connections 29.03.2026 13:27

Revenue: 30M\$

Community Connections operates as a non-profit behavioral health organization dedicated to serving vulnerable populations including women, men, youth, and children who face systemic barriers to healthcare access. The organization addresses critical gaps in mental health and substance use treatment by providing comprehensive services tailored to the specific needs of marginalized communities. The organization delivers an integrated continuum of care that combines behavioral health treatment, residential support services, and primary health care coordination.

14. Armed with the Private Information accessed in the Data Incidents (and a significant head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members’ names, taking out loans in Class Members’ names, using Class Members’ names to obtain medical services, using Class Members’ information to obtain government benefits, filing fraudulent tax returns using Class Members’ information, obtaining driver’s licenses in Class Members’ names but with another person’s photograph, and giving false information to police during an arrest.

15. There has been no assurance offered by Community Connections that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

*Ransomware Victim: Community Connections*, <https://www.redpacketsecurity.com/incransom-ransomware-victim-community-connections/> (last visited May 11, 2026); RANSOMLOOK, *Inc Ransom, Community Connections*, <https://www.ransomlook.io/group/inc%20ransom> (last visited May 11, 2026).

16. Therefore, Plaintiffs and other Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Incidents, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Incidents.

17. Plaintiffs bring this class action lawsuit to address Community Connections' inadequate safeguarding of their Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

18. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Community Connections, and thus Community Connections was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

19. Upon information and belief, Community Connections failed to properly monitor and/or properly implement timely security practices with regard to their systems that housed the Private Information of Plaintiffs and the Class. Had Community Connections properly monitored its networks, it would have discovered the Data Incidents sooner.

20. Plaintiffs and Class Members' identities are now at risk because of Community Connections' negligent conduct as the Private Information that Community Connections collected and maintained is now in the hands of data thieves and other unauthorized third parties.

21. Plaintiffs seek to remedy these harms on behalf of themselves, and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Incidents.

22. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, and declaratory judgment.

## II. PARTIES

23. Plaintiff **Paul Jefferson** is, and at all times mentioned herein was, an individual citizen of Washington, D.C.

24. Plaintiff **Evelyn Sands** is, and at all times mentioned herein was, an individual citizen of Washington, D.C.

25. Plaintiff **Bridgett Connor** is, and at all times mentioned herein was, an individual citizen of Silver Spring, Maryland.

26. Defendant **Community Connections** is a behavioral health agency incorporated in 1984 with its principal place of business located at 801 Pennsylvania Avenue, SE, Washington, D.C. 20003.

## III. JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action pursuant to Fla. Stat. § 26.012(2) because the amount in controversy exceeds \$50,000.00 exclusive of interest, costs, and attorney's fees.

28. This Court has personal jurisdiction over Defendant pursuant to Fla. Stat. §48.193(2) because Defendant is engaged in substantial and not isolated activity in this state.

29. Venue is proper in this County pursuant to Fla. Stat. § 47.051 because Defendant engages in business in Miami-Dade County and putative class members reside in this state, and a substantial part of the events giving rise to this action occurred in this County.

#### IV. FACTUAL ALLEGATIONS

##### ***A. Community Connections' Business and Collection of Plaintiffs' and Class Members' Private Information.***

30. Community Connections is a behavioral health provider that offers various services, including behavioral health, supportive housing, homeless outreach, and integrated health care coordination.<sup>7</sup>

31. Founded in 1984, Community Connections claims to be the largest not-for-profit behavioral health provider in the Nation's Capital and serves more than 3,000 patients annually.<sup>8</sup>

32. Community Connections employs more than 300 individuals and generates approximately \$32,448,224 in annual revenue.

33. As a condition of receiving behavioral health services and/or employment, Community Connections requires its patients and employees to entrust it with highly sensitive Private Information.

34. In the ordinary course of receiving service from Community Connections, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

35. Due to the highly sensitive and personal nature of the Private Information Community Connections acquires and stores with respect to its patients and employees, Community Connections, upon information and belief, promises to, among other things: (i) keep

---

<sup>7</sup> COMMUNITY CONNECTIONS, *Our Mission*, <https://communityconnectionsdc.org/mission> (last visited May 11, 2026).

<sup>8</sup> COMMUNITY CONNECTIONS, *Our History*, <https://communityconnectionsdc.org/history> (last visited May 11, 2026).

patients' and employees' Private Information private; (ii) comply with industry standards related to data security and the maintenance of its patients' and employees' Private Information; (iii) inform its patients and employees of its legal duties relating to data security and comply with all federal and state laws protecting patients' and employees' Private Information; (iv) only use and release patients' and employees' Private Information for reasons that relate to the services it provides; and (v) provide adequate notice to patients and employees if their Private Information is disclosed without authorization.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Community Connections assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

37. Plaintiffs and Class Members relied on Community Connections to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

***B. The First Data Incident and Defendant's Inadequate Notice to Plaintiffs and Class Members.***

38. According to Defendant's Notice Letters, Defendant learned of unauthorized access to its computer systems on October 21, 2024. However, the Notice Letters fail to state the precise dates the unauthorized access took place.

39. Through the First Data Incident, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, Social Security numbers, dates of birth, addresses, financial information, drivers' licenses and state ID information, medical information and health insurance information of at least 20,876 of individuals.

40. On or about August 28, 2025, roughly *ten (10) months* after Community Connections discovered the First Data Incident, Community Connections finally began notifying patients and employees that its investigation determined that their Private Information was exposed in the First Data Incident. Specifically, Community Connections sent Notice Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a “data security incident.”

41. Omitted from the Notice Letters are crucial details like: (i) the root cause of the First Data Incident; (ii) the date(s) of occurrence; (iii) the vulnerabilities exploited; and (iv) the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

42. Thus, Community Connections’ purported disclosure amounts to no real disclosure at all, because it fails to inform Plaintiffs and Class Members of the First Data Incident’s critical facts with any degree of specificity. Without these details, Plaintiffs and Class Members’ ability to mitigate the harms resulting from the First Data Incident was and is severely diminished.

43. In addition, the Notice Letters offer no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing twelve (12) months of complimentary credit monitoring—an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the First Data Incident

44. Community Connections had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs’ and

Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

45. Plaintiffs and Class Members provided their Private Information to Community Connections with the reasonable expectation and mutual understanding that Community Connections would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

46. Community Connections' data security obligations were particularly important given the substantial increase in cyberattacks in recent years, particularly among the healthcare industry.

47. Community Connections knew or should have known that its electronic records would be targeted by cybercriminals.

***C. The Second Data Incident and its Impact on Plaintiffs and Class Members.***

48. On or around April 4, 2026, Community Connections' systems were breached *again* through the Second Data Incident.<sup>9</sup>

49. According to online sources, the Second Data Incident was perpetrated by Inc Ransom ransomware group.<sup>10</sup>

50. Upon information and belief, due to Defendant's persistent negligence—resulting in the Second Data Incident—unauthorized cybercriminal(s) accessed a cache of highly sensitive

---

<sup>9</sup> See, e.g., HOOKPHISH (April 4, 2026), *Ransomware Group incransom Hits: Community Connections*, <https://www.hookphish.com/blog/ransomware-group-incransom-hits-community-connections/> (last visited May 11, 2026); REDPACKET SECURITY (April 4, 2026), *[INCRANSOM]—Ransomware Victim: Community Connections*, <https://www.redpacketsecurity.com/incransom-ransomware-victim-community-connections/> (last visited May 11, 2026); RANSOMLOOK, *Inc Ransom, Community Connections*, <https://www.ransomlook.io/group/inc%20ransom> (last visited May 11, 2026).

<sup>10</sup> *Id.*

Private Information, including names, Social Security numbers, dates of birth, addresses, financial information, drivers' licenses and state ID information, medical information and health insurance information of Plaintiffs and the Class.

51. Currently, the precise number of persons injured in the Second Data Incident is unknown. However, upon information and belief, the size of the putative class can be ascertained from documents and information in Community Connections' custody and control.

52. Upon information and belief, the number of victims of the Second Data Incident is comprised of thousands of individuals and the victims of the First Data Incident overlap with the victims of the Second Data Incident.

53. Upon information and belief, Plaintiffs are also victims of the Second Data Incident.

54. Defendant's negligence and inadequate data security speak for itself. Community Connections' inadequate data security practices caused yet *another* Data Incident only six (6) months after the First Data Incident.

55. Community Connections negligence is evidenced by its failure to prevent both the First Data Incident and the Second Data Incident. And thus, Community Connections caused widespread injury and monetary damages.

56. Upon information and belief, Community Connections has done little to remedy the vulnerabilities in its systems—as evidenced by two (2) data breaches in rapid succession. Thus, Plaintiffs' and Class Members' have no reasonable assurance that their Private Information will be protected from additional data breaches.

**D. *Because of Community Connections’ Second Data Incident, the Sensitive Private Information of Plaintiff and Class Members was Placed into the Hands of Cybercriminals—Inflicting Numerous Injuries and Significant Damages Upon Plaintiff and Class Members.***

57. Worryingly, online sources have reported that the cybercriminal ransomware group—Inc Ransom—has claimed responsibility for the Second Data Incident.<sup>11</sup>

58. Inc Ransom is a notorious, financially motivated cybercriminal group. The ransomware group has “a high level of technical expertise, employing advanced techniques and a multi-staged attack process to maximize their chances of success and the potential ransom payout.”<sup>12</sup> Inc Ransom “employs double extortion tactics (stealing sensitive data before encrypting systems) to maximize pressure on victims.”<sup>13</sup>

59. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking.”<sup>14</sup>

---

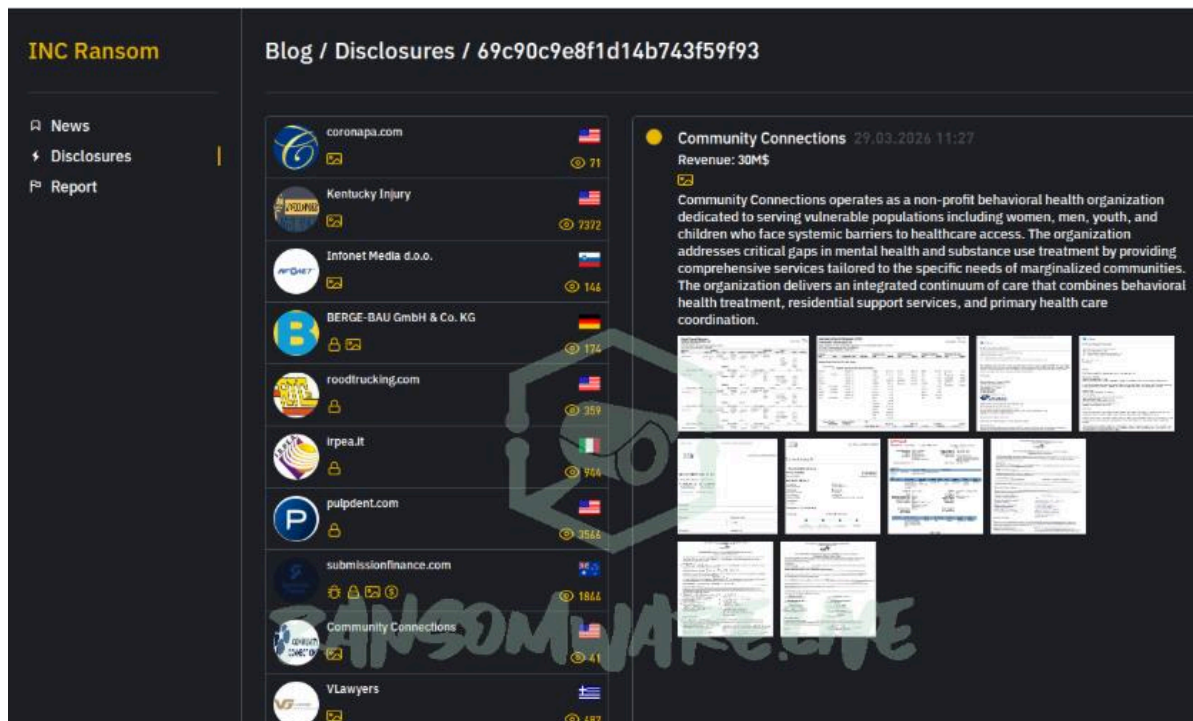
<sup>11</sup> *Id.*

<sup>12</sup> Gabby Lee, *INC Ransomware: Master of Double Extortion*, SECURITY DAILY REVIEW (June 10, 2025) <https://dailysecurityreview.com/resources/threat-actors-resources/inc-ransomware-master-of-double-extortion/>

<sup>13</sup> Laura Pompeu, *INC Ransomware: Tactics, Evolution, and Incident Response Guide*, PROVEN DATA (Jan. 26, 2026) <https://www.provenda.com/blog/inc-ransomware>

<sup>14</sup> Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

60. On or around April 4, 2026, Inc Ransom created a post on the Dark Web claiming that it hacked Community Connections.<sup>15</sup> A screenshot of Inc Ransom’s Dark Web post claiming responsibility for the Data is included below:



61. Inc Ransom’s Dark Web post included screenshots of documents exfiltrated from Community Connections’ computer system.

62. This indicates that Inc Ransom hacked Community Connections’ computer network, *stole* the sensitive Private Information contained therein, and will sell the stolen Private Information on the Dark Web.

63. Community Connections’ cyber and data security systems were completely inadequate in that it allowed cybercriminals to obtain files containing a treasure trove of Plaintiffs’ and the Class’s highly sensitive Private Information.

<sup>15</sup> *Community Connections, RANSOMWARE.LIVE*, <https://www.ransomware.live/id/Q29tbXVuaXR5IENvbm5lY3Rpb25zQGluY3JhbnNvbQ==> (last visited Apr. 8, 2026).

64. On information and belief, Community Connections has not made any public statements regarding Inc Ransom or whether it made a ransom payment.

65. However, even if Community Connections made a ransom payment, there is no guarantee that the Private Information *stolen* in the Second Data Incident will be deleted.<sup>16</sup> The stolen Private Information is valuable and can easily be sold to another threat actor, so there is little incentive to delete it.<sup>17</sup>

66. Thus, according to information and belief, Plaintiffs' and the Class's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

***E. The Healthcare Sector is Particularly Susceptible to Data Incidents.***

67. Community Connections was on notice that companies in the healthcare industry are highly susceptible targets for data breaches. Indeed, the First Data Incident should have made Defendant abundantly aware of this.

68. In August 2014, after a cyberattack on Community Health Systems, Inc., the Federal Bureau of Investigation ("FBI") warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."<sup>18</sup>

69. The American Medical Association ("AMA") has also warned healthcare

---

<sup>16</sup> Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, THE HIPPA JOURNAL (Feb. 23, 2024), <https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/>.

<sup>17</sup> *Id.*

<sup>18</sup> Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last visited May 11, 2026).

companies about the importance of protecting their patients' confidential information:

Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.<sup>19</sup>

70. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.<sup>20</sup> In 2022, the largest growth in compromises occurred in the healthcare sector.<sup>21</sup>

71. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident ... came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>22</sup>

72. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and

---

<sup>19</sup> Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N. (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (last visited May 11, 2026).

<sup>20</sup> IDENTITY THEFT RESOURCE CENTER, *2018 End-of-Year Data Breach Report*, [https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC\\_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf](https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf) (last visited May 11, 2026).

<sup>21</sup> IDENTITY THEFT RESOURCE CENTER, *2022 End-of-Year Data Breach Report*, [https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC\\_2022-Data-Breach-Report\\_Final-1.pdf](https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf) (last visited May 11, 2026).

<sup>22</sup> Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/> (last visited May 11, 2026).

identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.<sup>23</sup>

73. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”<sup>24</sup>

74. As a healthcare provider, Community Connections knew, or should have known, the importance of safeguarding its patients’ and employees’ Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Community Connections’ patients and employees as a result of a breach. Community Connections failed, however, to take adequate cybersecurity measures to prevent the Data Incidents from occurring.

#### ***F. Community Connections Failed to Comply with HIPAA.***

75. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq.* These provisions require that HHS create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

<sup>23</sup> *Id.*

<sup>24</sup> Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (April 4, 2019), <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited May 11, 2026).

76. Upon information and belief, Community Connections' Data Incidents resulted from a combination of insufficiencies that indicate Community Connections failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Community Connections' Data Incidents that Community Connections either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

77. Plaintiffs' and Class Members' Private Information compromised in the Data Incidents included "protected health information" as defined by CFR § 160.103.

78. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

79. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

80. Plaintiffs and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

81. Plaintiffs and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Incidents.

82. Based upon Defendant's Notice Letters to Plaintiffs and Class Members, Community Connections reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Incidents.

83. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incidents was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

84. Community Connections reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incidents was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

85. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incidents, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

86. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incidents.

87. Community Connections reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incidents.

88. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was exposed, acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Incidents, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

89. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered

unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

90. After receiving notice that they were victims of the Data Incidents (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

91. In addition, Community Connections' Data Incident could have been prevented if Community Connections had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

92. Community Connections' security failures also include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Community Connections creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to 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 rights in violation of 45 CFR 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and
- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

93. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400–414 also required Community Connections to provide notice of the Data Incidents to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach*” (emphasis added).

94. Because Community Connections has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Community Connections' approach to information security is adequate and appropriate going forward. Community Connections still maintains the Private Information of its

current and former patients and employees, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

**G. Community Connections Failed to Comply with FTC Guidelines.**

95. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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. Indeed, 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

96. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.<sup>25</sup> . The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

---

<sup>25</sup> *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), available at: [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited May 11, 2026).

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

98. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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, 15 U.S.C. § 45 *et seq.* Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

99. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like Community Connections here. *See, e.g., In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at \*32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

100. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Community Connections of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of Community Connections’ duty in this regard.

101. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated

that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.”<sup>26</sup>

102. As evidenced by the Data Incidents, Community Connections failed to properly implement basic data security practices. Community Connections’ failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs’ and Class Members’ Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

103. Community Connections was at all times fully aware of its obligation to protect the Private Information of its patients and employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

#### ***H. Community Connections Failed to Comply with Industry Standards.***

104. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

105. The Center for Internet Security’s (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability

---

<sup>26</sup> FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), transcript available at: [https://www.ftc.gov/sites/default/files/documents/public\\_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf) (last visited May 11, 2026).

Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.<sup>27</sup>

106. The National Institute of Standards and Technology (“NIST”) also recommends certain practices to safeguard systems, such as the following:

- a. Control who logs on to your network and uses your computers and other devices.
- b. Use security software to protect data.
- c. Encrypt sensitive data, at rest and in transit.
- d. Conduct regular backups of data.
- e. Update security software regularly, automating those updates if possible.
- f. Have formal policies for safely disposing of electronic files and old devices.
- g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

107. Further still, the United States Cybersecurity and Infrastructure Security Agency (“CISA”) makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that “remote access to the organization’s network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization’s IT personnel have disabled all ports and protocols that are not essential for business purposes,” and other steps; (b) taking steps to quickly detect a potential intrusion, including “[e]nsur[ing] that cybersecurity/IT

---

<sup>27</sup> *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, <https://www.cisecurity.org/controls/cis-controls-list> (last visited May 11, 2026).

personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization’s entire network is protected by antivirus/antimalware software and that signatures in these tools are updated,” and (c) “[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs,” and other steps.<sup>28</sup>

108. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs’ and Class Members’ Private Information, resulting in the Data Incidents.

***I. Community Connections Breached its Duty to Safeguard Plaintiffs’ and Class Members’ Private Information.***

109. In addition to its obligations under federal and state laws, Community Connections owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Community Connections owed a duty to Plaintiffs and Class Members to provide reasonable security, including

---

<sup>28</sup> *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/shields-guidance-organizations> (last visited May 11, 2026).

consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

110. Community Connections breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Community Connections' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect patients' and employees' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to sufficiently train its employees regarding the proper handling of its patients' and employees' Private Information;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and
- g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

111. Community Connections negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

112. Had Community Connections remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended

by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

113. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Incidents and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Community Connections.

***J. Plaintiffs and Class Members are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Incidents.***

114. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.<sup>29</sup> Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

115. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal 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 or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

---

<sup>29</sup> *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (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](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) (last visited May 11, 2026).

116. 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 to 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.

117. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

118. Thus, even if certain information was not purportedly involved in the Data Incidents, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

119. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

120. Cybercriminals can cross-reference two (2) sources of the Private Information compromised in the Data Incidents to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble

complete dossiers on individuals. These dossiers are known as “Fullz” packages.

121. The development of “Fullz” packages means that the stolen Private Information from the Data Incidents can easily be used to link and identify it to Plaintiffs’ and the proposed Class’s phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Incidents, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members’ stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Incidents.

122. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for seven (7) years if someone steals the victim’s identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.<sup>30</sup> However, these steps do not guarantee protection from identity theft but can only mitigate identity theft’s long-lasting negative impacts.

123. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank

---

<sup>30</sup> See FEDERAL TRADE COMMISSION, *IdentityTheft.gov*, <https://www.identitytheft.gov/Steps> (last visited May 11, 2026).

fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to 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, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

124. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.<sup>31</sup> After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding \$10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic or anxiety attacks.<sup>32</sup>

125. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.<sup>33</sup>

126. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

---

<sup>31</sup> IDENTITY THEFT RESOURCE CENTER, *2023 Consumer Impact Report* (Jan. 2024), [https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC\\_2023-Consumer-Impact-Report\\_Final-1.pdf](https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf) (last visited May 11, 2026).

<sup>32</sup> *Id.* at pp. 21–25.

<sup>33</sup> See FEDERAL TRADE COMMISSION, *What to Know About Identity Theft*, <https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last visited May 11, 2026).

127. While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, protected health information can sell for as much as \$363 according to the Infosec Institute.<sup>34</sup>

128. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

129. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "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. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."<sup>35</sup>

130. The ramifications of Community Connections' failure to keep its patients' and employees' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

131. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity

---

<sup>34</sup> CENTER FOR INTERNET SECURITY, *Data Breaches: In the Healthcare Sector*, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited May 11, 2026).

<sup>35</sup> Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), <https://kffhealthnews.org/news/rise-of-identity-theft/> (last visited May 11, 2026).

thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

132. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:<sup>36</sup>

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

133. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

134. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

#### ***K. Plaintiffs' and Class Members' Experiences and Damages.***

##### ***Plaintiff Paul Jefferson's Experience***

135. When Plaintiff Jefferson became a patient, Defendant required Plaintiff Jefferson to provide it with substantial amounts of his Private Information, including PHI.

---

<sup>36</sup> U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf> (last visited May 11, 2026).

136. On or about August 28, 2025, Plaintiff Jefferson received a Notice Letter from Defendant, which informed him that his Private Information had been accessed and acquired during the First Data Incident. The Notice Letter also informed him that the Private Information stolen included his name, Social Security number, financial information, driver's license or state identification information, medical information and health insurance information.

137. The Notice Letter offered Plaintiff Jefferson only twelve (12) months of complimentary credit monitoring services. One (1) year of credit monitoring is not sufficient given that Plaintiff Jefferson will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud, financial fraud, stolen identity, etc.

138. Upon information and belief, Plaintiff Jefferson's Private Information has also been accessed and acquired during the Second Data Incident.

139. Plaintiff Jefferson suffered actual injury in the form of time spent dealing with the Data Incidents and the increased risk of fraud resulting from the Data Incidents and/or monitoring his accounts for fraud.

140. Plaintiff Jefferson would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

141. Plaintiff Jefferson suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Incidents.

142. Plaintiff Jefferson suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information—a form of intangible property that

Plaintiff Jefferson entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Incidents.

143. Plaintiff Jefferson suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

144. Plaintiff Jefferson has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Community Connections fails to undertake the necessary and appropriate security and training measures to protect patients' and employees' Private Information.

145. As a result of the Data Incidents, Plaintiff Jefferson made reasonable efforts to mitigate the impact of the Data Incidents, including but not limited to researching the First Data Incident, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Jefferson has spent several hours dealing with the Data Incidents, valuable time he otherwise would have spent on other activities.

146. As a result of the Data Incidents, Plaintiff Jefferson has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him including, but not limited to, fraud and identity theft. Plaintiff Jefferson is very concerned about

this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Incidents would have on his life.

147. Plaintiff Jefferson also suffered actual injury from having his Private Information compromised as a result of the Data Incidents in the form of: (i) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Jefferson; (ii) violation of his privacy rights; and (iii) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

148. As a result of the Data Incidents, Plaintiff Jefferson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Incidents.

149. In sum, Plaintiff Jefferson and Class Members have been damaged by the compromise of their Private Information in the Data Incidents.

150. Further, Plaintiff Jefferson has already experienced instances in which his Private Information has been used to perpetuate fraud against him since the First Data Incident occurred. In September of 2025, Plaintiff Jefferson received a phone call from a debt collector that he was unfamiliar with, informing him that he was delinquent on payments for a line of credit taken out under his name for around \$1,000. This issue has yet to be resolved and has negatively impacted his credit score. This negative effect on his credit score has caused him duress and prevented Plaintiff Jefferson from being able to take out loans. It is reasonable for Plaintiff Jefferson to determine this instance of fraud was caused by the First Data Incident because this type of fraud can be perpetrated using the types of Private Information exposed in the First Data Incident.

151. Additionally, since the Data Incidents occurred, Plaintiff Jefferson has experienced multiple emails and alerts concerning suspicious login attempts to his accounts. Because of the

timing and nature of these suspicious activities using his Private Information, Plaintiff Jefferson believes that they are a result of his Private Information being exposed in the Data Incidents.

152. Plaintiff Jefferson and Class Members entrusted their Private Information to Defendant to receive Defendant's services. Their Private Information was subsequently compromised as a direct and proximate result of the Data Incidents, which resulted from Defendant's inadequate data security practices.

153. As a direct and proximate result of Community Connections' actions and omissions, Plaintiff Jefferson and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

154. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiff Jefferson and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the Data Incidents on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

155. Plaintiff Jefferson and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Incidents.

156. Plaintiff Jefferson and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private

Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff Jefferson and Class Members.

157. The Private Information stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff Jefferson and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff Jefferson and Class Members.

158. Additionally, Plaintiff Jefferson and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Incidents. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>37</sup> In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$50 a year.<sup>38</sup>

159. As a result of the Data Incidents, Plaintiff Jefferson's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff Jefferson or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff Jefferson and the Class Members, and because that data no longer

---

<sup>37</sup> See THE QUANTUM RECORD, *How Data Brokers Profit from the Data We Create*, <https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/> (last visited May 11, 2026).

<sup>38</sup> *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited May 11, 2026).

necessarily correlates only with activities undertaken by Plaintiff Jefferson and the Class Members, thereby causing additional loss of value.

160. Finally, Plaintiff Jefferson and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Incidents in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Incidents.

161. Moreover, Plaintiff Jefferson and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Community Connections, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

162. As a direct and proximate result of Community Connections' actions and inactions, Plaintiff Jefferson and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

***Plaintiff Evelyn Sands's Experience***

163. Plaintiff Sands was an employee of Defendant before the Data Incidents.

164. After Plaintiff Sands's employment ended, Defendant suffered the Data Incidents.

165. Plaintiff Sands was informed by Defendant that her Private Information may have been either accessed and/or acquired by an unauthorized individual including Plaintiff Sands's full or partial name, date of birth, government identification information, demographic information,

contact information, home address, financial information including, Social Security number, bank account number, health insurance information, and health information.

166. Plaintiff Sands is especially alarmed by the amount of stolen or accessed Private Information listed in Defendant's Notice Letter. Despite Defendant providing a list, she cannot be sure more of her PII or PHI was not exfiltrated. As a result of Defendant's First Data Incident, she now checks her bank accounts and credit cards throughout the day and spends approximately one (1) hour per week monitoring her accounts.

167. Upon information and belief, Plaintiff Sands' Private Information has also been accessed and acquired during the Second Data Incident.

168. Plaintiff Sands knows that cybercriminals often sell Private Information, and that her PII or PHI could be abused months or even years after a data breach. In this case, the cybercriminals affirmed they posted Plaintiff Sands's Private Information publicly.

169. Had Plaintiff Sands been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her Private Information.

170. To date, Defendant has not adequately compensated Plaintiff Sands and Class Members for the damages they sustained in the Data Incidents.

171. Defendant's failure to offer identity protective services is wholly inadequate as it fails to sufficiently compensate all victims of the Data Incidents, who commonly face multiple years of ongoing identity theft, and it entirely provides no compensation for its unauthorized release and disclosure of Plaintiff Sands's and Class Members' Private Information.

172. Furthermore, Defendant's credit monitoring advice to Plaintiff Sands and Class Members places the burden on Plaintiff Sands and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the First Data

Incident. Rather than automatically enrolling Plaintiff Sands and Class Members in years of credit monitoring services upon discovery of the October Breach, Defendant sent instructions to Plaintiff Sands and Class Members about actions they can affirmatively take to protect themselves.

173. Plaintiff Sands and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Incidents, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Incident.

174. Plaintiff Sands's Private Information was compromised and exfiltrated by cybercriminals as a direct and proximate result of the Data Incidents.

175. Plaintiff Sands was damaged in that her Private Information is in the hands of cybercriminals. As a direct and proximate result of Defendant's conduct, Plaintiff Sands and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

176. As a direct and proximate result of Defendant's conduct, Plaintiff Sands and Class Members have been forced to expend time dealing with the effects of the Data Incidents.

177. Plaintiff Sands and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

178. Plaintiff Sands and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff Sands and Class Members.

179. Plaintiff Sands and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Incidents.

180. Plaintiff Sands and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Incidents. Many courts have recognized the propriety of loss of value damages in related cases.

181. Plaintiff Sands and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

182. Plaintiff Sands and Class Members have suffered or will suffer actual injury as a direct result of the Data Incidents. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Incidents relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- f. Placing “freezes” and “alerts” with credit reporting agencies;
- g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- h. Contacting financial institutions and closing or modifying financial accounts;
- i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

- j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

183. Moreover, Plaintiff Sands and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password-protected.

184. Since the First Data Incident occurred, Plaintiff Sands has experienced a significant uptick in spam calls, emails, and messages using her Private Information. Specifically, Plaintiff Sands has experienced spam calls or texts related to medical appointments with unfamiliar doctors. Plaintiff Sands has also experienced suspicious login attempts to her accounts. Additionally, Plaintiff Sands received a dark web alert from Experian, CreditKarma, and Equifax informing her that her Private Information was found on the Dark Web. Shortly afterwards, Plaintiff Sands froze her credit to attempt to mitigate the damage that the First Data Incident has caused.

185. Further, because of Defendant's conduct, Plaintiff Sands and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

186. As a direct and proximate result of Defendant's actions and inactions, Plaintiff Sands and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

### ***Plaintiff Bridgett Connor's Experience***

187. Plaintiff Connor provided her Private Information to Defendant as a former patient. Plaintiff Connor greatly values her privacy and Private Information.

188. Prior to the Data Incidents, Plaintiff Connor took reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Connor would not have agreed to provide her Private Information to Defendant had Plaintiff Connor known that Defendant would not safeguard her Private Information from unauthorized access.

189. Plaintiff Connor is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

190. Plaintiff Connor received a Notice Letter dated August 28, 2025, from Defendant concerning the First Data Incident. The Notice Letter stated that unauthorized actors gained access to files on Defendant's network. The compromised files contained Plaintiff Connor's name, Social Security number, financial information, driver's license or state identification information, medical information, and health insurance information.

191. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Connor faces, Defendant offered her a one-year subscription to a credit monitoring service. Plaintiff Connor has not signed up for the program because she does not trust Defendant's chosen vendor with her Private Information. Additionally, Plaintiff Connor does not believe this is sufficient to protect her identity from the ongoing risks of theft she faces.

192. Upon information and belief, Plaintiff Connor's Private Information has also been accessed and acquired during the Second Data Incident.

193. Since learning of the Data Incidents and in an attempt to prevent the misuse of her Private Information, Plaintiff Connor has spent additional time reviewing her bank statements, credit cards, and reviewing her emails for fraud alerts.

194. Plaintiff Connor plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Incidents, including continually reviewing her depository, credit, and other accounts for any unauthorized activity. Indeed, Defendant's Notice Letter directs Plaintiff Connor to take such steps.

195. Since the First Data Incident occurred, Plaintiff Connor has experienced a significant uptick in spam calls, emails, and messages using her Private Information. Plaintiff Connor has also received spam calls and texts related to medical appointments with unfamiliar doctors. Additionally, Plaintiff Connor has experienced suspicious login attempts to her accounts, namely her Yahoo Mail account, since the First Data Incident occurred.

196. Plaintiff Connor has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

## **V. CLASS ACTION ALLEGATIONS**

197. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Florida Rules of Civil Procedure 1.220(a), (b)(2), and (b)(3).

198. Specifically, Plaintiffs propose the following Class (referred to herein as the "Class"), subject to amendment as appropriate:

### **Class**

All individuals in the United States whose Private Information was impacted as a result of the Data Incidents, including all individuals who were sent a Notice Letter.

199. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

200. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class, as well as the addition of any subclasses, before the Court determines whether certification is appropriate.

201. The proposed Class meets the criteria for certification under Florida Rules of Civil Procedure 1.220(a) and (b)(3).

202. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of at least approximately 20,876 patients and employees of Community Connections whose data was compromised in the Data Incidents. The identities of Class Members are ascertainable through Community Connections' records, Class Members' records, publication notice, self-identification, and other means.

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

- a. Whether Community Connections engaged in the conduct alleged herein;
- b. Whether Community Connections' conduct violated the FTCA and/or HIPAA;
- c. When Community Connections learned of the Data Incidents;

- d. Whether Community Connections' response to the Data Incidents was adequate;
- e. Whether Community Connections unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
- f. Whether Community Connections failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Incidents;
- g. Whether Community Connections' data security systems prior to and during the Data Incidents complied with applicable data security laws and regulations;
- h. Whether Community Connections' data security systems prior to and during the Data Incidents were consistent with industry standards;
- i. Whether Community Connections owed a duty to Class Members to safeguard their Private Information;
- j. Whether Community Connections breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Incidents;
- l. Whether Community Connections had a legal duty to provide timely and accurate notice of the Data Incidents to Plaintiffs and the Class Members;
- m. Whether Community Connections breached its duty to provide timely and accurate notice of the Data Incidents to Plaintiffs and Class Members;

- n. Whether Community Connections knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiffs and Class Members suffered as a result of Community Connections' misconduct;
- p. Whether Community Connections' conduct was negligent;
- q. Whether Community Connections' conduct was *per se* negligent;
- r. Whether Community Connections was unjustly enriched;
- s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

204. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Incidents. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Community Connections. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

205. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

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

208. Class certification is also appropriate under Florida Rules of Civil Procedure 1.220(b)(2). Community Connections has acted and/or refused to act on grounds generally

applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

209. Finally, all members of the proposed Class are readily ascertainable. Community Connections has access to the names and addresses and/or email addresses of Class Members affected by the Data Incidents. Class Members have already been preliminarily identified and sent notice of the First Data Incident by Community Connections.

## **VI. CLAIMS FOR RELIEF**

### **COUNT I NEGLIGENCE (ON BEHALF OF PLAINTIFFS AND THE CLASS)**

210. Plaintiffs restate and reallege the allegations stated in paragraphs 1 through 209 as if fully set forth herein.

211. Community Connections knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

212. Community Connections' duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

213. Community Connections knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Community Connections was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

214. Community Connections owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Community Connections' duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect patients' and employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;
- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. To promptly notify Plaintiffs and Class Members of the Data Incidents, and to precisely disclose the type(s) of information compromised.

215. Community Connections' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

216. Community Connections' duty also arose because Defendant was bound by industry standards to protect its patients' and employees' confidential Private Information.

217. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Community Connections owed them a duty of care to not subject them to an unreasonable risk of harm.

218. Community Connections, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Community Connections' possession.

219. Community Connections, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

220. Community Connections, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Incidents and then failing to provide prompt notice of the Data Incidents to the persons whose Private Information was compromised.

221. Community Connections breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;

- e. Failing to comply with the FTCA;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Incidents so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

222. Community Connections had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Community Connections with their Private Information was predicated on the understanding that Community Connections would take adequate security precautions. Moreover, only Community Connections had the ability to protect its systems (and the Private Information that it stored on them) from attack.

223. Community Connections' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

224. As a result of Community Connections' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

225. Community Connections' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

226. As a result of Community Connections' negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in

that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

227. Community Connections also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Incidents.

228. As a direct and proximate result of Community Connections' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

229. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

230. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

231. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Community Connections to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

**COUNT II**  
**BREACH OF IMPLIED CONTRACT**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

232. Plaintiffs restate and reallege the allegations stated in paragraphs 1 through 209 as if fully set forth herein.

233. Community Connections provides behavioral health services and/or employment. Plaintiffs and Class Members formed implied contracts with Defendant regarding the provision of those services/employment through their collective conduct, including by Plaintiffs and Class

Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services/employment.

234. Through Defendant's provision of services/employment to Plaintiffs and Class Members, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its internal policies, practices, and applicable law.

235. As consideration, Plaintiffs and Class Members paid money to Community Connections and/or turned over valuable Private Information to Community Connections. Accordingly, Plaintiffs and Class Members bargained with Community Connections to securely maintain and store their Private Information.

236. Community Connections accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services/employment to Plaintiffs and Class Members.

237. By paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's services/employment, Plaintiffs and Class Members intended and understood that Community Connections would adequately safeguard the Private Information as part of those services/employment.

238. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to: (i) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (ii) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (iii) restricting access to qualified and trained employees and/or agents; (iv) designing and implementing appropriate retention policies to protect the Private Information against criminal

data breaches; (v) applying or requiring proper encryption; (vi) implementing multifactor authentication for access; (vii) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (viii) taking other steps to protect against foreseeable data breaches.

239. Plaintiffs and Class Members would not have entrusted their Private Information to Community Connections in the absence of such an implied contract.

240. Had Community Connections disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Community Connections.

241. As a provider of behavioral healthcare, Community Connections recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

242. Community Connections violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Community Connections further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

243. Additionally, Community Connections breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

244. Community Connections also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems

that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

245. Community Connections further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

246. Community Connections further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

247. Community Connections further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

248. Community Connections further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

249. Community Connections further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

250. Community Connections further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health

information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

251. Community Connections further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

252. Community Connections further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

253. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to Community Connections in exchange for Community Connections' agreement to, *inter alia*, provide services/employment that included protection of their highly sensitive Private Information.

254. Plaintiffs and Class Members have been damaged by Community Connections' conduct, including the harms and injuries arising from the Data Incidents now and in the future, as alleged herein.

**COUNT III  
UNJUST ENRICHMENT  
(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

255. Plaintiffs restate and reallege the allegations stated in paragraphs 1 through 209 as if fully set forth herein.

256. This Count is plead in the alternative to Count II.

257. Plaintiffs and Class Members conferred a benefit on Community Connections by turning over their Private Information to Defendant and by paying for services/providing labor that

allowed Defendant to obtain revenue. This should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

258. Upon information and belief, Community Connections funds its data security measures entirely from its general revenue, including payments made to it by Plaintiffs and Class Members.

259. As such, a portion of this should have been used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Community Connections.

260. Community Connections has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

261. Community Connections knew that Plaintiffs and Class Members conferred a benefit upon it, which Community Connections accepted. Community Connections profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Incidents.

262. If Plaintiffs and Class Members had known that Community Connections had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

263. Due to Community Connections' conduct alleged herein, it would be unjust and inequitable under the circumstances for Community Connections to be permitted to retain the benefit of its wrongful conduct.

264. As a direct and proximate result of Community Connections' conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Incidents, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Community Connections' possession and is subject to further unauthorized disclosures so long as Community Connections fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Incidents for the remainder of the lives of Plaintiffs and Class Members.

265. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Community Connections and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Community Connections from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

266. Plaintiffs and Class Members may not have an adequate remedy at law against Community Connections, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**COUNT IV**  
**BREACH OF FIDUCIARY DUTY**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

267. Plaintiffs restate and reallege the allegations stated in paragraphs 1 through 209 as if fully set forth herein.

268. In light of the special relationship between Community Connections and its patients and employees, whereby Community Connections became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) Community Connections was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients and employees, including Plaintiffs and Class Members. This benefit included: (i) the safeguarding of Plaintiffs' and Class Members' Private Information; (ii) timely notifying Plaintiffs and Class Members of the Data Incidents; and (iii) maintaining complete and accurate records of what and where Community Connections' patients' and employees' Private Information was and is stored.

269. Community Connections had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its relationship with patients and employees, in particular to keep the Private Information secure.

270. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Incidents to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

271. Community Connections breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

272. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Community Connections created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

273. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

274. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

275. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

276. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

277. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

278. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

279. Community Connections breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

280. As a direct and proximate result of Community Connections' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

## **VII. PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

- a. An order certifying this action as a Class action under Florida Rules of Civil Procedure 1.220, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;
- b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

- d. An order instructing Community Connections to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
- e. An order requiring Community Connections to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

#### **VIII. DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury on all triable issues.

DATED: May 11, 2026

Respectfully submitted,

By: /s/Tonyia Johnson  
Tonyia Johnson (FBN 1058251)  
**SHAMIS & GENTILE P.A.**  
tjohnson@shamisgentile.com  
14 NE 1st Ave., Suite 705  
Miami, Florida 33132  
Tel: (305) 479-2299

***Counsel for Plaintiffs and the Class***