

# Supreme Court of Pennsylvania

Court of Common Pleas  
 Cecil B. Yocum Street

LACKAWANNA County



For Prothonotary Use Only:

Docket No:

23-cv-3008

TIME STAMP

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

**Commencement of Action:**

- Complaint       Writ of Summons       Petition  
 Transfer from Another Jurisdiction       Declaration of Taking

Lead Plaintiff's Name:

Yvonne Ayala

Lead Defendant's Name:

Commonwealth Health Physician Network, dba Great Valley Cardiology, and Scranton Cardiovascular Physician Services, LLC

Are money damages requested?  Yes     No

Dollar Amount Requested:  
(check one)

- within arbitration limits  
 outside arbitration limits

Is this a *Class Action Suit*?     Yes     No

Is this an *MDJ Appeal*?     Yes     No

Name of Plaintiff/Appellant's Attorney: Francesca Kester Burne

Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)

**Nature of the Case:** Place an "X" to the left of the **ONE** case category that most accurately describes your **PRIMARY CASE**. If you are making more than one type of claim, check the one that you consider most important.

**TORT** (do not include Mass Tort)

- Intentional  
 Malicious Prosecution  
 Motor Vehicle  
 Nuisance  
 Premises Liability  
 Product Liability (does not include mass tort)  
 Slander/Libel/ Defamation  
 Other: \_\_\_\_\_

**CONTRACT** (do not include Judgments)

- Buyer Plaintiff  
 Debt Collection: Credit Card  
 Debt Collection: Other \_\_\_\_\_  
 Employment Dispute: Discrimination  
 Employment Dispute: Other \_\_\_\_\_  
 Other: \_\_\_\_\_

**CIVIL APPEALS**

- Administrative Agencies
- Board of Assessment  
 Board of Elections  
 Dept. of Transportation  
 Statutory Appeal: Other \_\_\_\_\_  
 Zoning Board  
 Other: \_\_\_\_\_

**MASS TORT**

- Asbestos  
 Tobacco  
 Toxic Tort - DES  
 Toxic Tort - Implant  
 Toxic Waste  
 Other: Negligence

**REAL PROPERTY**

- Ejectment  
 Eminent Domain/Condemnation  
 Ground Rent  
 Landlord/Tenant Dispute  
 Mortgage Foreclosure: Residential  
 Mortgage Foreclosure: Commercial  
 Partition  
 Quiet Title  
 Other: \_\_\_\_\_

**MISCELLANEOUS**

- Common Law/Statutory Arbitration  
 Declaratory Judgment  
 Mandamus  
 Non-Domestic Relations Restraining Order  
 Quo Warranto  
 Replevin  
 Other: \_\_\_\_\_

**PROFESSIONAL LIABILITY**

- Dental  
 Legal  
 Medical  
 Other Professional: \_\_\_\_\_

**IN THE COURT OF COMMON PLEAS OF LACKAWANNA COUNTY**

YVONNE AYALA,  
individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

COMMONWEALTH HEALTH  
PHYSICIAN NETWORK, dba GREAT  
VALLEY CARDIOLOGY and SCRANTON  
CARDIOVASCULAR PHYSICIAN  
SERVICES, LLC

Defendants.

Case No. 2023-cv- 3008

CIVIL ACTION – CLASS  
ACTION

JURY TRIAL DEMANDED

MAURICE KELLY  
LACKAWANNA COUNTY  
CLERK OF JUDICIAL  
RECORDS & COURT REPORTING  
10/01/23 11 A 013

**NOTICE**

You have been sued in Court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this Complaint and Notice are served, by entering a written appearance personally or by an attorney and filing in writing with the Court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the Court without further notice for any money claimed in the Complaint or for any other claim or relief requested by the Plaintiff. You may lose property or other rights important to you.

**YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE.  
IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO  
OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT  
WHERE YOU CAN GET LEGAL HELP.**

**NORTHERN PENNSYLVANIA  
LEGAL SERVICES, INC.**  
33 N. Main Street, Suite 200  
Pittston, PA 18640  
Telephone: (570) 299-4100

**LAWYER REFERRAL SERVICE**  
Lackawanna Bar Association  
338 N. Washington Avenue  
Scranton, PA 18503-1502  
Telephone: (570) 969-9600

**IN THE COURT OF COMMON PLEAS OF LACKAWANNA COUNTY**

YVONNE AYALA,  
individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

COMMONWEALTH HEALTH  
PHYSICIAN NETWORK, dba GREAT  
VALLEY CARDIOLOGY and SCRANTON  
CARDIOVASCULAR PHYSICIAN  
SERVICES, LLC

Defendants.

Case No. 2023-cv- 3008

CIVIL ACTION – CLASS  
ACTION

JURY TRIAL DEMANDED

MAINTENANCE  
LACKAWANNA COUNTY  
2023 JUN 17 A 3:14  
CLERK OF JUDICIAL  
RECORDS CIVIL DIVISION

**CLASS ACTION COMPLAINT**

NOW COMES, Plaintiff Yvonne Ayala, individually and on behalf of the Class defined below of similarly situated persons, who brings this Class Action Complaint and alleges the following against Commonwealth Health Physician Network, doing business as Great Valley Cardiology, and Scranton Cardiovascular Physician Services, LLC (collectively “Defendants” or “GVC”) based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

**NATURE OF THE ACTION**

1. Plaintiff brings this class action against Defendants for Defendants’

failure to properly secure and safeguard protected health information (“PHI”) as defined by the Health Insurance Portability and Accountability Act (“HIPAA”), medical information, and other personally identifiable information (“PII”), including without limitation names, addresses, demographic information such as dates of birth, Social Security numbers, drivers’ license numbers, passport numbers, credit card and debit card information, bank account information, health insurance information and health insurance claims information, dates of service, diagnoses, medications, lab results, and other treatment information (collectively, “Private Information”), for failing to comply with industry standards to protect information systems that contain that Private Information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their Private Information had been compromised. Plaintiff seeks, among other things, orders requiring Defendants to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future.

2. GVC is a leading, multi-specialty group healthcare provider with locations throughout northeastern Pennsylvania.

3. On or about June 12, 2023, GVC announced a data security incident that occurred between February 2, 2023, and April 14, 2023, involving Private Information (the “Data Breach”). The Data Breach was wide-reaching and

compromised the PHI of over 181,000 individuals, according to the submission GVC made to the U.S. Secretary of Health and Human Services at the Office for Civil Rights (“OCR”).<sup>1</sup>

4. GVC also began notifying, via U.S. Mail, affected individuals including certain current and former patients on June 12, 2023.

5. This case involves a breach by an unknown third party, resulting in the unauthorized disclosure of the Private Information of Plaintiff and Class Members by GVC to unknown third parties. As a result of GVC’s failure to implement and follow basic security procedures, Plaintiff’s and Class Members’ Private Information is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to GVC’s failures.

6. Additionally, as a result of GVC’s failure to follow contractually agreed upon, federally prescribed, industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services GVC was to provide. GVC expressly represented that it would maintain the confidentiality of Plaintiff and

---

<sup>1</sup> Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last accessed July 2, 2023).

Class Members' Private Information obtained throughout the course of treatment.

7. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence, negligence per se, breach of implied contract, and breach of fiduciary duty.

### **PARTIES**

8. Plaintiff is a citizen and resident of Scranton, Pennsylvania. Plaintiff was a patient of GVC. Plaintiff's Private Information was disclosed without authorization to an unknown third party as a result of the Data Breach.

9. Defendant Commonwealth Health Physician Network - Cardiology is a company with its principal place of business at 743 Jefferson Avenue, Scranton, Pennsylvania, 18510. On information and belief, Scranton Cardiovascular Physician Services, LLC is a part of Commonwealth Health Physician Network and maintains offices at the same address.

10. GVC cares for individuals through a network of facilities, primary and specialty care practices located in the Commonwealth of Pennsylvania. Due to the nature of these services, GVC collects and electronically stores Private Information.

### **JURISDICTION AND VENUE**

11. The Court of Common Pleas of Lackawanna County, Pennsylvania has subject matter jurisdiction over this matter pursuant to 42 Pa. C.S.A. § 931.

12. This Court has personal jurisdiction over GVC pursuant to 42 Pa. C.S.A. § 530(2) because GVC maintains its principal place of business in this jurisdiction and is authorized to and does conduct substantial business in this jurisdiction.

13. Venue is proper in this Court because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this County, GVC is based in this County, GVC maintains patients' Private Information in this County, and GVC has caused harm to Plaintiff and Class Members residing in this County.

### **FACTUAL BACKGROUND**

#### ***A. Defendants' Business***

14. Commonwealth Health Physician Network is a multi-specialty group with locations throughout Luzerne, Lackawanna, and Wayne Counties.

15. Commonwealth Health Physician Network represents a wide variety of different specialties, including cardiology.

16. Patients regularly provide Private Information to Defendants in the course of receiving medical care.

17. As a healthcare provider, Defendants are required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without the patients' express written consent, as further detailed below.

## ***B. The Data Breach***

18. On April 13, 2023, GVC identified a security incident that resulted in the exposure of sensitive, private information to unauthorized individuals.<sup>2</sup>

19. After conducting an investigation, GVC determined that unauthorized third parties gained access to GVC's computer network between February 2, 2023 and April 14, 2023.

20. The investigation concluded that through this unauthorized access, the unauthorized third party had access to sensitive patient Private Information including at least: names, addresses, demographic information such as dates of birth, drivers' license numbers, passport numbers, credit card and debit card information, bank account information, health insurance information and health insurance claims information, dates of service, diagnoses, medications, lab results, and other treatment information.

21. GVC concluded that patient Social Security numbers were also compromised.

22. On or about June 12, 2023, GVC began mailing letters to affected individuals whose information was identified as compromised.

---

<sup>2</sup> See <https://www.cwhphysiciannetwork.net/security-incident> (last accessed July 10, 2023).



23. The letters Plaintiff and Class Members received were untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive patient information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether GVC knows if the data has not been further disseminated.

24. GVC downplayed the seriousness of the incident by telling Plaintiff and Class Members that they cannot determine whether the unauthorized parties viewed or took the personal information to which they had access.

25. These representations are boilerplate language suggesting GVC's lack of concern for the seriousness of the Data Breach—wherein an unauthorized third party gained access to Private Information in GVC's possession.

26. To date, GVC has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, GVC has taken to secure the Private Information still in its possession.

27. Through this litigation, Plaintiff and Class Members seek to determine the scope of the Data Breach and the information involved, obtain relief that redresses Plaintiff's and Class Members' harms, and ensure GVC has proper measures in place to prevent another breach from occurring in the future.

### ***C. The Healthcare Sector is Particularly Susceptible to Data Breaches***

28. GVC was on notice that companies in the healthcare industry are susceptible targets for data breaches.

29. GVC was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, nearly ten years ago, after a cyberattack on Community Health Systems, Inc., the FBI began warning 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>3</sup>

30. Healthcare data breaches have since skyrocketed. 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>4</sup> Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential.

31. 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

---

<sup>3</sup> Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), available at: <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last accessed Jun. 16, 2023).

<sup>4</sup> Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at: <https://www.idtheftcenter.org/2018-data-breaches/> (last accessed Jun. 16, 2023).

the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>5</sup> 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 identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.<sup>6</sup>

32. 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>7</sup>

33. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

---

<sup>5</sup> Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed Jun. 16, 2023).

<sup>6</sup> *Id.*

<sup>7</sup> Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at: <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last accessed Jun. 16, 2023).

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>8</sup>

34. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"<sup>9</sup>

35. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."<sup>10</sup>

---

<sup>8</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 Jun. 16, 2023).

<sup>9</sup> Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results* (Mar. 27, 2019), <https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results> (last visited Jun. 16, 2023).

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

36. As a major healthcare provider, GVC knew, or should have known, the importance of safeguarding the patients' Private Information entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on GVC's patients as a result of a breach. GVC failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

***D. GVC Obtains, Collects, and Stores Plaintiff's and Class Members' PHI***

37. GVC obtains, collects, and stores a massive amount of its patients' protected health information and personally identifiable data.

38. As a condition of engaging in health services, GVC requires that patients entrust it with highly confidential Private Information.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, GVC assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' Private Information from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and, as current and former patients, they rely on GVC to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

### ***E. The Value of Private Information and the Effects of Disclosure***

41. GVC was well aware that the information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

42. PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.<sup>11</sup> 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.

43. While credit card information and associated personally identifiable information 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>12</sup>

44. 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.

---

<sup>11</sup> Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last accessed Jun. 16, 2023).

<sup>12</sup> Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at: <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last accessed Jun. 16, 2023).

45. Medical identify 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>13</sup>

46. The ramifications of GVC's failure to keep its patients' PHI secure are long lasting and severe. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

47. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.<sup>14</sup> This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they

---

<sup>13</sup> Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: <https://khn.org/news/rise-of-identity-theft/> (last accessed Jun. 16, 2023).

<sup>14</sup> See Medical ID Theft Checklist, *available at*: <https://www.identityforce.com/blog/medical-id-theft-checklist-2> (last accessed Jun. 16, 2023).

received collection letters from creditors for expenses that were incurred in their names.<sup>15</sup>

48. Here, not only was sensitive medical information compromised, but also financial information and Social Security numbers. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.<sup>16</sup> This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

49. Stolen Social Security numbers make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of

---

<sup>15</sup> Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, available at: <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf> (last accessed Jun. 16, 2023).

<sup>16</sup> *Identity Theft and Your Social Security Number*, Social Security Administrative available at <http://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jun. 16, 2023).



the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

50. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

51. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>17</sup>

52. GVC knew, or should have known, the importance of safeguarding its patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on GVC's patients as a result of a breach. GVC failed, however,

---

<sup>17</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Jun. 16, 2023).

to take adequate cybersecurity measures to prevent the Data Breach from occurring, creating long lasting and severe ramifications.

***F. Plaintiff and Class Members Have Suffered Damages***

53. Plaintiff is a patient of Commonwealth Health Network. On or about June 12, 2023, Plaintiff received notification in the mail that her name, address, phone number, health plan number, health plan claims information, medical record number, and other medical information were compromised in the Data Breach.

54. This unauthorized access disturbs Plaintiff as she no longer has control over her highly sensitive medical records, cannot stop others from viewing them, and cannot prevent criminals from misusing them.

55. What's more, the Data Breach exposed Plaintiff to a substantially increased lifelong risk for identity theft and fraud. Indeed, the Data Breach included her most sensitive medical information.

56. Plaintiff has already spent several hours of her time attempting to mitigate the harm caused by the Data Breach. She anticipates spending considerable additional time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

57. Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

58. Plaintiff suffers a present injury from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals. Plaintiff has a continuing interest in ensuring that her PII and PHI, which is the type that cannot be changed and upon information and belief remains in Defendant's possession, is protected and safeguarded from future breaches.

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

60. Despite all of the publicly available knowledge of the continued compromises of Private Information, GVC's approach to maintaining the privacy of GVC's patients' protected health information was lackadaisical, cavalier, reckless, or in the very least, negligent.

61. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of GVC's misfeasance.

62. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches

are more likely to become victims of identity fraud.<sup>18</sup>

63. GVC's delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

64. As a result of GVC's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;
- b. Unauthorized use and misuse of their PHI;
- c. The loss of the opportunity to control how their PHI is used;
- d. The diminution in value of their PHI;
- e. The compromise, publication, and/or theft of their PHI;
- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate

---

<sup>18</sup> 2014 LexisNexis True Cost of Fraud Study, available at: <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last accessed Jun. 16, 2023).

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies;
- j. The diminished value of GVC's goods and services they received;
- k. Lost opportunity and benefits of electronically filing of income tax returns;
- l. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- m. The continued risk to their Private Information, which remains in the possession of GVC and is subject to further breaches so long as GVC fails to undertake appropriate measures to protect the Private Information in its possession; and
- n. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

***G. GVC's Conduct Violates HIPAA***

65. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PHI like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

66. GVC’s Data Breach resulted from a combination of insufficiencies that indicate GVC failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from GVC’s Data Breach that GVC either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff’s and Class Members’ PHI.

67. Plaintiff’s and Class Members’ Private Information is “protected health information” as defined by 45 CFR § 160.103.

68. 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.”

69. 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[.]”

70. Plaintiff’s and Class Members’ Private Information is “unsecured protected health information” as defined by 45 CFR § 164.402.

71. Plaintiff’s and Class Members’ unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

72. Based upon the breach notification letter, GVC reasonably believes Plaintiff’s and Class Members’ unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

73. Plaintiff’s and Class Members’ unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

74. GVC reasonably believes Plaintiff’s and Class Members’ unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

75. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

76. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

77. It is reasonable to infer that Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

78. It should be rebuttably presumed that unsecured protected health information acquired, accessed, used, 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.

79. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this



case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

80. In addition, GVC's Data Breach could have been prevented if GVC 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.

81. GVC's 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 GVC 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; 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);
- g. 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);
- h. 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);
- i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);
- j. 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.*

82. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required GVC to provide notice of the breach to each affected individual "without unreasonable delay and *in no case later than 60 days following discovery of the*

*breach.*<sup>19</sup>

83. Because GVC has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure GVC's approach to information security is adequate and appropriate. GVC still maintains the protected health information and other sensitive information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent Data Breaches.

#### ***H. GVC Failed to Comply with FTC Guidelines***

84. GVC was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

85. The Federal Trade Commission ("FTC") has promulgated guides for businesses that highlight the importance of implementing reasonable data security

---

<sup>19</sup> Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at: [hhs.gov/hipaa/for-professionals/breach-notification/index.html](https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html)* (emphasis added) (last visited Jun. 16, 2023).

practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>20</sup>

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.<sup>21</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.

87. The FTC further recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>22</sup>

88. The FTC has brought enforcement actions against businesses for failing

---

<sup>20</sup> Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Jan. 16, 2023).

<sup>21</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, 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 accessed Jan. 16, 2023).

<sup>22</sup> FTC, *Start With Security*, *supra* note 16.

to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. GVC failed to properly implement basic data security practices. GVC’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patients’ Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. GVC was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a leading healthcare provider. GVC was also aware of the significant repercussions that would result from its failure to do so.

### **CLASS ACTION ALLEGATIONS**

91. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated pursuant to the Pennsylvania Rules of Civil Procedure.

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

**All individuals whose Private Information was compromised in the GVC Data Breach announced by GVC on or about June 12, 2023.**

93. Excluded from the Class are the officers, directors, and legal representatives of GVC, and the judges and court personnel in this case and any members of their immediate families.

94. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to plaintiff.

95. Numerosity. The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of at least 181,000 patients.

96. 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 and to what extent Defendants had a duty to protect the Private Information of Class Members;
- b. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' Private Information;
- c. Whether Defendants had duties not to disclose the Private Information of Class Members to unauthorized third parties;
- d. Whether Defendants took reasonable steps and measures to safeguard

### Plaintiff's and Class Members' Private Information

- e. Whether Defendants failed to adequately safeguard the Private Information of Class Members;
- f. Whether Defendants breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' Private Information by storing that information on unsecured servers;
- g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiff and Class Members on the other;
- i. Whether Defendants had respective duties not to use the Private Information of Class Members for non-business purposes;
- j. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- k. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendants' wrongful conduct;

- o. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;
- p. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and
- q. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

97. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was disclosed by GVC. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of GVC. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

98. Policies Generally Applicable to the Class. This class action is also appropriate for certification because GVC has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole.



GVC's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on GVC's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

99. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation and in particular privacy class litigation, and Plaintiff intends to prosecute this action vigorously.

100. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like

GVC. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

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

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

105. Further, GVC has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

**FIRST CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of Plaintiff and the Class)**

106. Plaintiff realleges paragraphs 1 through 105 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

107. As a condition of receiving medical care from GVC, patients were obligated to provide GVC with certain Private Information, including their dates of birth, Social Security numbers, financial information, personal medical information, and other protected health information.

108. Plaintiff and the Class Members entrusted their Private Information to GVC on the premise and with the understanding that GVC would safeguard their information, use their Private Information for business or medical purposes only, and/or not disclose their Private Information to unauthorized third parties.

109. GVC has full knowledge of the sensitivity of Private Information and

the types of harm that Plaintiff and Class Members could and would suffer if Private Information was wrongfully disclosed.

110. GVC knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of patients' Private Information involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

111. GVC had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing GVC's security protocols to ensure that Plaintiff's and Class Members' information in GVC's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of patients' personal and medical information.

112. GVC had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' Private Information.

113. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of the growing amount of data breaches for health care providers and other industries.

114. Plaintiff and Class Members were the foreseeable and probable victims

of any inadequate security practices and procedures. GVC knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and that it had inadequate employee training and education and IT security protocols in place to secure the Private Information of Plaintiff and the Class.

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

116. Plaintiff and the Class Members had no ability to protect their Private Information that was in GVC's possession.

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

118. GVC had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and Class Members within GVC's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow

Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

119. GVC has admitted that the Private Information of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

120. GVC, through its actions and/or omissions, unlawfully breached GVC's duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and Class Members during the time the Private Information was within GVC's possession or control.

121. GVC improperly and inadequately safeguarded the Private Information of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

122. GVC, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' Private Information.

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

124. But for GVC's wrongful and negligent breach of duties owed to

Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

125. There is a close causal connection between GVC's failure to implement security measures to protect the Private Information of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' Private Information was accessed as the proximate result of GVC's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

126. As a direct and proximate result of GVC's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their 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, tax fraud, 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in GVC's possession and is subject to further unauthorized disclosures

so long as GVC fails to undertake appropriate and adequate measures to protect the Private Information of patients and former patients in its continued possession; (viii) 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 Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of GVC's goods and services Plaintiff and Class Members received.

**SECOND CAUSE OF ACTION**  
**Negligence *per se***  
**(On Behalf of Plaintiff and the Class)**

127. Plaintiff realleges paragraphs 1 through 105 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

128. Violation of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury constitute negligence *per se*.

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

130. GVC violated Section 5 of the FTC Act by failing to use reasonable



measures to protect Plaintiff's and Class Members' Private Information and not complying with applicable industry standards, as described in detail herein. GVC's conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

131. GVC's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

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

134. GVC's violations of HIPAA also independently constitute negligence *per se*.

135. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA

privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

136. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

137. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

138. As a direct and proximate result of GVC's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their 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, tax fraud, 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in GVC's possession and is subject

to further unauthorized disclosures so long as GVC fails to undertake appropriate and adequate measures to protect the Private Information of patients and former patients in its continued possession; (viii) 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 Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of GVC's goods and services Plaintiff and Class Members received.

**THIRD CAUSE OF ACTION  
Breach of Implied Contract  
(On Behalf of Plaintiff and the Class)**

139. Plaintiff realleges paragraphs 1 through 105 above as if fully set forth herein.

140. Plaintiff and Class Members were required to provide their Private Information, including names, Social Security numbers, dates of birth, medical histories, and other personal information to GVC as a condition of receiving medical care from GVC.

141. Plaintiff and Class Members paid money to GVC in exchange for goods and services, as well as GVC's promises and obligations to protect Private Information from unauthorized disclosure.

142. By providing public healthcare services, Defendants promised Plaintiff and Class Members that Defendants would only disclose protected health

information and sensitive information under certain circumstances, none of which relate to the Data Breach.

143. By providing public healthcare services, Defendants promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' protected health information would remain protected.

144. Implicit in the agreement between GVC's patients, including Plaintiff and Class Members, to provide Private Information, and GVC's acceptance of such Private Information, was GVC's obligation to use the Private Information of its patients for business purposes only, take reasonable steps to secure and safeguard that Private Information, and not make unauthorized disclosures of the Private Information to unauthorized third parties.

145. Further, implicit in the agreement, GVC was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other Private Information.

146. Without such implied contracts, Plaintiff and Class Members would not have provided their Private Information to GVC.

147. GVC had an implied duty to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

148. Plaintiff and Class Members fully performed their obligations under the implied contract with GVC; however, GVC did not.

149. GVC breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' Private Information, which was compromised as a result of the Data Breach.

150. GVC further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA.

151. GVC further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information GVC created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

152. GVC further breached the implied contracts with Plaintiff and Class Members by 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).

153. GVC further breached the implied contracts with Plaintiff 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).

154. GVC further breached the implied contracts with Plaintiff 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).

155. GVC further breached the implied contracts with Plaintiff 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).

156. GVC further breached the implied contracts with Plaintiff 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).

157. GVC further breached the implied contracts with Plaintiff 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).

158. GVC further breached the implied contracts with Plaintiff 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.*

159. GVC further breached the implied contracts with Plaintiff and Class

Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

160. GVC further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PHI.

161. GVC's failures to meet these promises constitute breaches of the implied contracts.

162. Because GVC allowed unauthorized access to Plaintiff's and Class Members' PHI and failed to safeguard the Private Information, GVC breached its contracts with Plaintiff and Class Members.

163. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay GVC in exchange for GVC's agreement to, *inter alia*, protect their PHI.

164. GVC breached its contracts by not meeting the minimum level of protection of Plaintiff's and Class Members' PHI.

165. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in GVC providing goods and services to Plaintiff and Class Members that were of a diminished value.

166. As a direct and proximate result of GVC's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have

suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their 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, tax fraud, 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in GVC's possession and is subject to further unauthorized disclosures so long as GVC fails to undertake appropriate and adequate measures to protect the Private Information of customers/patients and former customers/patients in its continued possession; (viii) 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 Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of GVC's goods and services they received.

167. As a direct and proximate result of GVC's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have



suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**FOURTH CAUSE OF ACTION**  
**Breach of Fiduciary Duty**  
**(On Behalf of Plaintiff and the Class)**

168. Plaintiff realleges paragraphs 1 through 105 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

169. In light of the special relationship between GVC and its patients, whereby GVC became a guardian of Plaintiff's and Class Members' highly sensitive, confidential, personal, financial information, and other Private Information, GVC was a fiduciary, created by its undertaking and guardianship of the PHI, to act primarily for the benefit of its patients, including Plaintiff and Class Members, for: (1) the safeguarding of Plaintiff's and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of a data breach or disclosure; and (3) maintaining complete and accurate records of what and where GVC's patients' information was and is stored.

170. GVC had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular to keep secure the Private Information of its patients.

171. GVC breached its fiduciary duties to Plaintiff and Class Members by

failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

172. GVC breached its fiduciary duties to Plaintiff and Class Members by failing to protect Plaintiff's and Class Members' Private Information.

173. GVC breached its fiduciary duties to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

174. GVC breached its fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information GVC created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

175. GVC breached its fiduciary duties to Plaintiff and Class Members by 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).

176. GVC breached its fiduciary duties to Plaintiff 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).

177. GVC breached its fiduciary duties to Plaintiff 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).

178. GVC breached its fiduciary duties to Plaintiff 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).

179. GVC breached its fiduciary duties to Plaintiff 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).

180. GVC breached its fiduciary duties to Plaintiff 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).

181. GVC breached its fiduciary duties to Plaintiff 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.*

182. As a direct and proximate result of GVC's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their

PHI 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, tax fraud, 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in GVC's possession and is subject to further unauthorized disclosures so long as GVC fails to undertake appropriate and adequate measures to protect the Private Information of customers/patients and former customers/patients in its continued possession; (viii) 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 Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of GVC's goods and services they received.

183. As a direct and proximate result of GVC's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

## **PRAYER FOR RELIEF**

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

- a. For an Order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;
- b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- c. For equitable relief compelling Defendants to use appropriate cyber security methods and policies with respect to Private Information collection, storage, and protection, to disclose with specificity to Class Members the type of Private Information compromised and enjoining Defendants' conduct requiring it to implement proper data security practices, specifically:
  - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all

- applicable regulations, industry standards, and laws;
- iii. requiring Defendants to delete, destroy, and purge the Private Information of Plaintiff and the Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class members;
  - iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and the Class members' Private Information;
  - v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
  - vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
  - vii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

- viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- ix. requiring Defendants to conduct regular database scanning and securing checks;
- x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI, as well as protecting the Private Information of Plaintiff and the Class members;
- xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs,

- and systems for protecting Private Information;
- xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
  - xiv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;
  - xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;
  - xvi. requiring Defendants to design, maintain, and test its computer systems to ensure that PII/PHI in its possession is adequately secured and protected;
  - xvii. requiring Defendants to disclose any future data breaches in a timely and accurate manner;
  - xix. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and
  - xx. requiring Defendants to provide lifetime credit monitoring and identity



theft repair services to Class members.

- d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
- e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- f. For prejudgment interest on all amounts awarded; and
- g. Such other and further relief as this Court may deem just and proper.

### **DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a trial by jury on all issues so triable.

Respectfully submitted,

Date: July 14, 2023

BY:

s/ Francesca Kester Burne

**MORGAN & MORGAN**

**COMPLEX LITIGATION GROUP**

Francesca Kester Burne, PA Bar No. 324523

Jean S. Martin \*

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

Telephone: (813) 318-5189

Facsimile: (813) 222-2496

[fburne@forthepeople.com](mailto:fburne@forthepeople.com)

[jeanmartin@forthepeople.com](mailto:jeanmartin@forthepeople.com)

\*to seek admission *pro hac vice*

***Attorneys for Plaintiff and the Proposed Class***

RINALDI & POVEROMO, P.C.

BY: 

Carl J. Poveromo

PA Attorney ID No. 44713

P.O. Box 826

520 Biden Street

Scranton, PA 18501-0826

Telephone: (570) 346-7441

Facsimile: (570) 346-8170

cjp@lawinpa.com

***Local Counsel for Plaintiff and the  
Proposed Class***

I VERIFY that the statements made in this Complaint are true and correct. I understand that false statements herein are made subject to the penalties of 18 Pa. C. S. § 4904, relating to unsworn falsification to authorities.

\_\_\_\_\_

Date: 7/13/2023

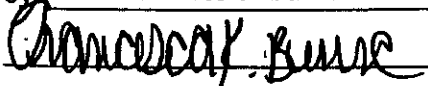
*[date of verification]*

Yvonne Ayala

*[signature of plaintiff]*

**CERTIFICATE OF COMPLIANCE**

I certify that this filing complies with the provisions of the *Case Records Public Access Policy of the Unified Judicial System of Pennsylvania* that require filing confidential information and documents differently than non-confidential information and documents.

Submitted by: Francesca Kester Burne  
Signature:   
Name: Francesca Kester Burne  
Attorney No. (if applicable): 324523

MAURI B. KELLY  
SACRAWANNA COUNTY  
2023 JUL 17 A 10:15  
CLERK OF JUDICIAL  
RECORDS CIVIL DIVISION