GOLOMB & HONIK, P.C.
KENNETH J. GRUNFELD, ESQUIRE
Identification No.: 84121
RICHARD GOLOMB, ESQUIRE
1835 Market Street, Suite 2900
Philadelphia, PA 19104
(215) 985-9177
kgrunfeld@golombhonik.com

GARY F. LYNCH, ESQUIRE
KELLY IVERSON, ESQUIRE
CARLSON LYNCH, LLP
1133 Penn Ave., Fl. 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com

MAJOR JURY CASE

CLASS ACTION
ASSESSMENT OF DAMAGES HEARING IS REQUIRED

Attorney for Plaintiffs

SIMONA OPRIS, ADRIAN ADAM and BRITNEY RICHARDSON, on behalf of themselves and all others similarly situated,

Plaintiff,

v.

SINCERA REPRODUCTIVE MEDICINE, formerly known as and operating as ABINGTON REPRODUCTIVE MEDICINE, P.C.

Defendant.

IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY

TERM, 2021

NO:

CLASS ACTION COMPLAINT

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 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 complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las paginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificacion. Hace falta asentar una comparencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su persona. Sea avisado que si usted no se defiende, la corte tomara medidas y puede continuar la demanda en contra suya sin previo aviso o nofificacion. Ademas, la corte puede decidir a favor del demandante y requiere que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades y otros derechos importantes para usted.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP

Lawyer Reference Service
Philadelphia Bar Association
1101 Market Street, 11th Floor
Philadelphia, PA 19107
(215) 238-6300

LLEVE ESTA DEMANDA A UN ABOGADO IMMEDIATAMENTE. SI NO TIENE ABOGADO O SI NO TIENE EL DINERO SUFICIENTE DE PAGAR TAL SERVICO. VAYA EN PERSONA O LLAME POR TELEFONO A LA OFICINA CUYA DIRECCION SE ENCUENTRA ESCRITA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL.

Lawyer Reference Service
Philadelphia Bar Association
1101 Market Street, 11th Floor
Philadelphia, PA 19107
(215) 238-6300

Plaintiffs Simona Opris, Adrian Adam and Britney Richardson ("Plaintiffs") bring this Class Action Complaint on behalf of themselves and all others similarly situated, against Defendant**,** Sincera Reproductive Medicine, formerly known as and operating as Abington Reproductive Medicine, P.C. ("Sincera" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data breach manifests in several ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take several additional prophylactic measures.

3. As a healthcare provider, Sincera is required by law to provide every patient with a Notice of Privacy Practices. In its HIPPA [sic] Notice of Privacy Practices, Sincera advises its patients that: "[w]e are required by law to maintain the privacy of protected health information."[1]

4. Under federal law, Sincera must provide notice to patients within 60 days of discovering an inappropriate use or disclosure of protected health information.

5. Sincera knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

6. Plaintiffs bring this class action on behalf of individuals, patients of or people that are customers of or have their records at Sincera whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach of Sincera's network server, which Sincera states occurred between August 10, 2020 and September 13, 2020 (the "Data Breach").

7. Despite that Sincera became aware of the Data Breach by September 11, 2020, it failed to notify Plaintiffs and the putative Class Members within 60 days as required by law. Notably, Sincera failed to notify Plaintiffs of the Data Breach for more than eight months from its discovery of the same.

8. Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence, breach of fiduciary duty, violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and declaratory judgment, seeking actual and punitive damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of Sincera to date, a wide variety of PII and PHI was implicated in the breach, including, but not limited to: names, social security numbers, dates of birth, medical records or patient account numbers, health insurance information, and/or treatment or clinical information, such as diagnosis, medications, provider, type of treatment, or treatment locations.

[1] https://sincerareproductive.com/wp-content/uploads/2020/11/HIPPA-form.docx (last visited 5/27/2021).

10. As a direct and proximate result of Sincera's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiffs' and Class Members' PII and/or PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

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

12. To recover from Sincera for these harms, Plaintiffs and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Sincera to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Sincera; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

13. Plaintiff Simona Opris is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Pennsylvania. On or about May 13, 2021, Plaintiff Opris received a written notification from Defendant informing Plaintiff Opris that her PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach. Plaintiff Opris is married to Plaintiff Adam.

14. Plaintiff Adrian Adam is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Pennsylvania. On or about May 13, 2021, Plaintiff Adam received a written notification from Defendant informing Plaintiff Adam that his Social Security number, PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach. Plaintiff Adam is married to Plaintiff Opris.

15. Plaintiff Britney Richardson is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Pennsylvania. On or about May 13, 2021, Plaintiff Richardson received a written notification from Defendant informing Plaintiff Ricardson that her PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach.

16. Defendant Sincera Reproductive Medicine ("Sincera") brands itself as an entity that was formerly known as Abington Reproductive Medicine. https://sincerareproductive.com/ (last visited 5/27/2021). Upon information and belief, this entity is still listed with the PA Department of State, Corporation Bureau as Abington Reproductive Medicine, P.C., a Pennsylvania Professional Corporation with a principal place of business at 1245 Highland Avenue, Suite 404 in Abington, Pennsylvania 19001.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action pursuant to 42 Pa. C.S.A. § 931 and 73 Pa. Stat. Ann. § 201-9.2.

18. The Court has personal jurisdiction over Defendant pursuant to 42 Pa. C.S.A. § 5301.

19. Venue in Philadelphia County is proper pursuant to Pa. R.C.P. No. 2179(a) because it is where Plaintiff Richardson resides; where Defendant regularly advertises and markets its services and conducts business; and where the cause of action arose.

FACTUAL BACKGROUND

A. Sincera Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

20. At all relevant times, Sincera knew it was storing and permitting its employees to use its internal network server to transmit valuable, sensitive PII and PHI and that, as a result, Sincera's systems would be attractive targets for cybercriminals.

21. Sincera also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

22. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

23. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[2] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

24. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the IRTC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[3]

---

[2] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited 5/27/2021).

[3] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection (last visited 5/27/2021).

25. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[4]

26. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[5]

27. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[6]

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

29. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[7] A complete identity theft kit that includes health insurance credentials may be

---

[4] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1) (last visited 5/27/2021).

[5] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited 5/27/2021).

[6] *Id.*

[7] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited 5/27/2021).

worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[8]

30. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[9]

31. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

[8] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com /gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited 5/27/2021).

[9] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited 5/27/2021).

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[10]

32. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Sincera Breached its Duty to Protect its Patients PII and PHI

33. On September 11, 2020, Sincera identified suspicious activity relating to its internal network server.

34. According to Sincera, it hired incident response and forensic specialists to assist it with its investigation, which it completed by April 22, 2021. [11]

35. The investigation revealed that the hacker had gained access to the accounts by August 10, 2020. Sincera did not contain the breach until September 13, 2020 – meaning the hacker had unlimited access to patient data on its networks (including Plaintiffs' and Class Members' breached PII and PHI) for nearly five weeks.

36. The patient PII and PHI exposed in the Data Breach included names, driver's license numbers, medical diagnosis and/or medical treatment information, prescription information, treating/referring physician information, other treatment information, and health insurance information.

[10] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf (last visited 5/27/2021).

[11] https://www.prnewswire.com/news-releases/Sincera-reproductive-medicine-provides-notice-of-data-security-incident-301292695.html (last visited 5/27/2021).

37. On or before November 8, 2020, the Maze ransomware site, located on the dark web, listed "Abington Reproductive Medicine," Sincera's former name, as a recent cyberattack victim.[12]

38. Maze is a site where cyberattackers post data stolen from victims, including PII and PHI, in order to pressure victims to pay ransom demands.[13]

39. Sincera reported the Data Breach to HHS on December 3, 2020, more than three months after the Data Breach began and more than two months after Sincera became aware of it.

40. All in all, more than 37,000 patients of Sincera had their PII and/or PHI breached.[14]

41. The Data Breach occurred as a direct result of Sincera's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' PII and PHI.

42. Plaintiffs received notices from Sincera dated May 13, 2021, advising that Plaintiffs were victims of Sincera's data security failures exposing Plaintiffs' names, driver's license numbers, medical diagnosis and/or medical treatment information, prescription information, treating/referring physician information, other treatment information, and health insurance information.to criminal hackers. The Notices are attached as Exhibits A, B and C.

43. Like Plaintiffs, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

44. In its notice to Plaintiffs and Class members, Sincera asserted: "In response to this incident, we moved swiftly to confirm the security of our internal systems and to prevent continued unauthorized access to our network."

---

[12] https://www.databreaches.net/wp-content/uploads/Without_Undue_Delay.pdf (last visited 5/27/2021).

[13] *Id.*

[14] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited 5/27/2021).

45. Sincera issued a press release dated May 17, 2021 acknowledging the Data Breach.[15]

C. Plaintiff and Class Members Suffered Damages

46. For the reasons mentioned above, Sincera's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

47. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Sincera's conduct. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

48. As a result of Sincera's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PHI.

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

[15] https://www.prnewswire.com/news-releases/Sincera-reproductive-medicine-provides-notice-of-data-security-incident-301292695.html (last visited 5/27/2021).

CLASS ALLEGATIONS

50. Plaintiffs bring this case individually and, pursuant to Rules 1702, 1708, and 1709 of the Pennsylvania Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII and/or PHI was compromised in the Sincera data breach which occurred starting in August 2020 (the "Class").

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

52. Plaintiffs reserve the right to modify or amend the definition of the proposed Class prior to moving for class certification.

53. **Numerosity – Pennsylvania Rule of Civil Procedure 1702(1).** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Based on public information, the Class includes tens of thousands of individuals.

54. **Commonality – Pennsylvania Rule of Civil Procedure 1702(2).** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

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

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Defendant breached its fiduciary duty to Plaintiffs and the Class.

d. Whether Defendant violated the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 Pa. Stat. § 201-1, *et seq.*;

e. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

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

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

55. **Typicality – Pennsylvania Rule of Civil Procedure 1702(3)**. Plaintiffs' claims are typical of the claims of the Class Members. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PHI. Plaintiffs and Class Members were all patients of Sincera, each having their PII and PHI obtained by an unauthorized third party.

56. **Adequacy of Representation – Pennsylvania Rule of Civil Procedure 1702(4) and 1709.** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

57. **Predominance – Pennsylvania Rule of Civil Procedure 1708(a)(1).** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure PII and PHI on its network server, then Plaintiffs and each Class Member suffered damages from the exposure of their sensitive personal information in the Data Breach.

58. **Manageability – Pennsylvania Rule of Civil Procedure 1708(a)(2).** While the precise size of the Class is unknown without the disclosure of Defendants' records, public records indicate at least 37,000 individuals whose PII and/or PHI was compromised in the Data Breach. The claims of Plaintiffs and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Class.

59. **Risk of Inconsistent, Varying or Prejudicial Adjudications – Pennsylvania Rule of Civil Procedure 1708(a)(3).** If the claims of Plaintiffs and the members of the Class were tried separately, Defendants may be confronted with incompatible standards of conduct and divergent court decisions. Furthermore, if the claims of Plaintiffs and the members of the Class were tried individually, adjudications with respect to individual Class Members and the propriety of their claims could be dispositive on the interests of other members of the Class not party to those individual adjudications and substantially, if not fully, impair or impede their ability to protect their interests.

60. **Litigation Already Commenced – Pennsylvania Rule of Civil Procedure 1708(a)(4)**. To Plaintiffs' knowledge, there are no other cases that have been brought against Defendants, or that are currently pending against Defendants, where a Pennsylvania consumer seeks to represent a class of Pennsylvania residents based on the conduct alleged in this Class Action Complaint.

61. **The Appropriateness of the Forum – Pennsylvania Rule of Civil Procedure 1708(a)(5).** This is the most appropriate forum to concentrate the litigation because Plaintiff Richardson resides in this county, the Defendant advertises and markets services and does business in the county, and a substantial number of Class Members were injured in this County.

62. **The Class Members' Claims Support Certification – Pennsylvania Rule of Civil Procedure 1708(a)(6) and (7)**. Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits.

Furthermore, the damages that may be recovered by the Class will not be so small such that class certification is unjustified.

63. **The General Applicability of Defendant's Conduct – Pennsylvania Rule of Civil Procedure 1708(b)(2)**. Defendant's failure to secure PII and PHI is generally applicable to the Class as a whole, making equitable and declaratory relief appropriate with respect to each Class Member.

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

64. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

65. Sincera owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

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

67. Sincera had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Sincera was obligated to act with reasonable care to protect against these foreseeable threats.

68. Sincera's duty also arose from Sincera's position as a provider of healthcare. Sincera holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Sincera, as a direct healthcare provider, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

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

70. But for Sincera's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

71. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Sincera or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Sincera's duty.

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

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

74. Sincera's violation of Section 5 of the FTC Act constitutes negligence *per se*.

75. The harm that has occurred as a result of Sincera's conduct is the type of harm that the FTC Act was intended to guard against.

76. Sincera is an entity covered under the Health Insurance Portability and Accountability Act ("HIPAA"), which sets minimum federal standards for privacy and security of PHI.

77. Pursuant to HIPAA, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations, Sincera had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiffs' and the Class Members' electronic PHI.

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

79. HIPAA also requires Sincera to provide Plaintiff and the Class Members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 CFR §§ 164.400-414.

80. Sincera violated HIPAA by actively disclosing Plaintiffs' and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to provide Plaintiffs and Class Members with notification of the Data Breach within 60 days after its discovery.

81. Plaintiffs and the Class Members are patients within the class of persons HIPAA was intended to protect.

82. Sincera's violation of HIPAA constitutes negligence *per se*.

83. The harm that has occurred as a result of Sincera's conduct is the type of harm that HIPAA was intended to guard against.

84. Pursuant to Pennsylvania's Policies and Procedures for Medical Records Services, 28 Pa. Code § 115.1, *et. seq*. (the "Pa. Policies"), Sincera was required to have a medical record

service "properly equipped to enable its personnel to function in an effective manner and to maintain medical records so that they are readily accessible and secure from unauthorized use."

85. It was also required to train its medical record service personnel. *Id.*

86. Additionally, Sincera was required to store medical records "in such a manner as to provide protection from loss, damage and unauthorized access." *Id.*

87. Pursuant to the Pa. Policies, Sincera was required to treat "all records" (including those of Plaintiff's and the Class Members) "as confidential." *Id.*

88. Sincera violated the Pa. Policies by actively disclosing Plaintiffs' and the Class Members' PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI; and failing to maintain the confidentiality of Plaintiffs' and the Class Members' records.

89. Plaintiffs and the Class Members are patients within the class of persons the Pa. Policies was intended to protect.

90. Sincera's violation of the Pa. Policies constitutes negligence *per se*.

91. The harm that has occurred as a result of Sincera's conduct is the type of harm that the Pa. Policies were intended to guard against.

92. As a direct and proximate result of Sincera's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

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

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

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future

consequences of the Sincera Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

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

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Sincera with the mutual understanding that Sincera would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

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

93. As a direct and proximate result of Sincera's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

94. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

95. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Sincera and that was ultimately accessed or compromised in the Data Breach.

96. As a healthcare provider, Sincera has a fiduciary relationship to its patients, like Plaintiffs and the Class Members.

97. Because of that fiduciary and special relationship, Sincera was provided with and stored private and valuable PHI related to Plaintiffs and the Class.

98. Sincera owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

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

100. But for Sincera's wrongful breach of its duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

101. As a direct and proximate result of Sincera's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

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

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

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

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

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Sincera with the mutual understanding that Sincera would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

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

102. As a direct and proximate result of Sincera's breach of its fiduciary duty, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 P.S. §§ 201-1, et seq.

103. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

104. Sincera is a "person," as meant by 73 P.S. § 201-2(2).

105. Plaintiffs and Class Members purchased goods and/or services from Sincera primarily for personal, family and/or household purposes.

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

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201-2(4)(vii));

c. Failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made (73 P.S. § 201-2(4)(xiv)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

107. Defendant's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures in response to increasing cybersecurity risks in the healthcare sector, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42

U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505;

f. Failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;

g. Misrepresenting that certain sensitive PII and PHI was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII and PHI; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with the common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505.

108. Sincera's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Class Members, about the adequacy of Sincera's data security and ability to protect the confidentiality of consumers' PII and PHI.

109. Sincera's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Class Members, leading them to

believe for several months that their PII and PHI was secure and that they did not need to take actions to secure their identities.

110. Sincera intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

111. Had Sincera disclosed to Plaintiffs and Class Members that its network systems were not secure and thus vulnerable to attack, Sincera would have been forced to adopt reasonable data security measures and comply with the law. Instead, Plaintiffs and Class Members entrusted Sincera with their sensitive and valuable PII and PHI. Sincera accepted the responsibility of being a steward of this data, while keeping the inadequacy of its security measures secret from the public. Accordingly, because Sincera held itself out as maintaining a secure system for PII and PHI data, Plaintiffs and Class Members acted reasonably in relying on Sincera's misrepresentations and omissions, the truth of which they could not have discovered.

112. Sincera acted intentionally, knowingly, willfully, wantonly, maliciously, and outrageously to violate Pennsylvania's Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Class Members' rights.

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

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

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

115. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

116. Under 42 P.S. § 7532, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

117. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Sincera is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Sincera's data security measures remain inadequate, contrary to Sincera's assertion that it has confirmed the security of its network. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

118. Pursuant to its authority under 42 P.S. § 7532, this Court should enter a judgment declaring, among other things, the following:

a. Sincera owes a legal duty to secure PII and PHI and to timely notify patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes; and

b. Sincera continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

119. This Court also should issue corresponding prospective injunctive relief requiring Sincera to employ adequate security protocols consistent with law and industry standards to protect PII and PHI.

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

121. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Sincera if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Sincera of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Sincera has a pre-existing legal obligation to employ such measures.

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

PRAYER FOR RELIEF

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

a. For an order certifying the Class under Rule 1702 of the Pennsylvania Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

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

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

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

e. Declaratory and injunctive relief as described herein;

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

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

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

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June1, 2021

Respectfully Submitted,

KENNETH J. GRUNFELD, ESQUIRE
GOLOMB & HONIK, P.C.
1835 Market Street, Suite 2900
Philadelphia, Pennsylvania 19103
Telephone: (215) 346-7338
Facsimile: (215) 985-4169
rgolomb@GolombHonik.Com
KGrunfeld@GolombHonik.Com

/s/ Gary F. Lynch
Gary F. Lynch, Esquire
Kelly Iverson, Esquire
CARLSON LYNCH, LLP
1133 Penn Ave., Fl. 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com

Counsel for Plaintiff

V E R I F I C A T I O N

KENNETH J. GRUNFELD, ESQUIRE, hereby states that he is counsel for Plaintiffs in this action and verifies that the statements made in the foregoing Complaint are true and correct to the best of his knowledge, information and belief and that this verification is made with the knowledge, permission and consent of Plaintiffs. Counsel takes this verification for the purpose of assuring the timely filing of this Complaint. The verification of the party-plaintiffs' will be substituted at a later date. The undersigned understands that the statements therein are made subject to penalties of 18 Pa. C.S.A. Section 4904 relating to unsworn falsification to authorities.

DATED: June 1, 2021

KENNETH J. GRUNFELD, ESQUIRE
Attorney for Plaintiff