UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

Case No.: _____

JAMES LANDINI and KAELA MARIE PERRY, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

CIRCLES OF CARE, INC., a Florida not for profit corporation,

Defendant.

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs JAMES LANDINI and KAELA MARIE PERRY (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant CIRCLES OF CARE, INC. ("COC" or "Defendant"), based upon personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

NATURE OF THE ACTION

1. On or around September 6, 2022, COC had its data servers breached by unauthorized third-party hackers, who stole the highly sensitive personal and medication information—including, *inter alia*, the first and last names, dates of birth, social security numbers, addresses, phone numbers, driver's license numbers, bank routing and accounting numbers, medical account numbers, provider names, service dates, diagnoses, and medical procedure codes—of approximately 61,170 of COC's patients.[1]

2. COC is one of the leading behavioral health care providers in facilities, services, budget and professional staff in the State of Florida.[2] As a requirement to procure its services, COC requires that its patients provide COC with their Personal Identifying Information ("PII") and Protected Health Information ("PHI"). As a result, COC collects and stores the PII and PHI of tens of thousands of individuals who have utilized its services.

3. Under statute and regulation, COC had a duty to implement reasonable, adequate industry-standard data security policies safeguards to protect patient PII and PHI. COC failed to do so. COC expressly recognizes those duties in its public-facing Privacy Policy, wherein it states that "[w]e at Circles of Care respect your

[1] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed January 31, 2023).
[2] https://www.circlesofcare.org/about/philosophy-history-2/ (last accessed January 31, 2023).

privacy. This is part of our code of ethics. We are required by law to maintain the privacy of 'protected health information' about you, to notify you of our legal duties and your legal rights, and to follow the privacy policies described in this notice."[3] Despite this, COC did not obtain its patients' consent before allowing their information to be accessed and exfiltrated by unauthorized third-party hackers.

4. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter "Class Members"), bring this Class Action to secure redress against COC for its reckless and negligent violation of their privacy rights. Plaintiffs and Class Members are patients and former patients of COC who had their PII and PHI collected, stored and ultimately breached by COC.

5. Plaintiffs and Class Members have suffered injuries and damages. As a result of COC's wrongful actions and inactions, Plaintiffs and Class Members' PII and PHI have all been compromised. Plaintiffs and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and credit fraud for the remainder of their lifetimes. Plaintiffs and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts and the purchase of credit monitoring services, to protect themselves from future loss. Plaintiffs and Class Members have

[3] *Privacy Policy*, https://www.circlesofcare.org/about/privacy-policy-2/ (last accessed January 31, 2023).

also lost the value of their PII and PHI.

6. As a result of COC's wrongful actions and inactions, patient information was stolen. Plaintiffs and Class Members who have had their PHI/PII compromised by nefarious third-party hackers, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Plaintiffs and Class Members bring this action to secure redress against COC.

THE PARTIES

7. Plaintiff James Landini ("Landini") is a Florida citizen residing in Melbourne, Florida. Landini is a former patient of COC. On or around December 29, 2022, Landini received a data breach notice from COC informing him that his PII and PHI had been implicated in the data breach.

8. Plaintiff Kaela Marie Perry ("Perry") is a Florida citizen residing in Melbourne, Florida. Perry is a former patient of COC. On or around December 29, 2022, Perry received a data breach notice from COC informing her that her PII and PHI had been implicated in the data breach.

9. COC is a Florida not for profit corporation with its principal place of business located at 400 East Sheridan Road, Melbourne, Florida 32901. Defendant's registered agent for service of process is David L. Feldman, who is located at that same address.

JURISDICTION AND VENUE

10. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331 for claims that arise under the Stored Communications Act, 18 U.S.C. § 2701, *et seq*. The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state claims because they are so related to the federal claims in that they form a part of the same case or controversy.

11. Additionally, this Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because upon the original filing of this complaint, putative Class Members reside in states around the country; there are more than 100 putative Class Members; and the amount in controversy exceeds $5 million.

12. The Court also has personal jurisdiction over Defendant because it routinely conducts business in the state of Florida and has sufficient minimum contacts in Florida to have intentionally availed itself to this jurisdiction by operating and marketing its services in Florida.

13. Venue is proper in this District because, among other things: (a) Plaintiffs are residents of this District and citizens of this state; (b) Defendant is a resident of this District and directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District for services provided in this district.

14. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because, among other things: (a) Plaintiffs reside in the Middle District, (b) Defendant conducts substantial business in the Middle District, (c) Defendant directed its services at residents in the Middle District; and (d) many of the acts and omissions that give rise to this Action took place in the Middle District.

FACTUAL ALLEGATIONS

A. The Data Breach

15. COC is a HIPAA healthcare provider, as well as one of the leading behavioral health centers in the state of Florida. As a requirement to procure its services, COC requires its patients to provide it with their sensitive PII and PHI. As a result, COC's systems store the PII and PHI of tens and thousands of patients who have utilized its medical services.

16. On or around September 6, 2022 COC's systems were accessed by unauthorized third-party hackers, who exfiltrated Plaintiffs' and Class Members' sensitive PII and PHI— including, *inter alia*, the first and last names, dates of birth, social security numbers, addresses, phone numbers, driver's license numbers, bank routing and accounting numbers, medical account numbers, provider names, service

dates, diagnoses, and medical procedure codes—of approximately 61,170 of its patients.[4]

17. This data breach was the direct result of COC's failure to implement reasonable and adequate data security safeguards, as required by statute and regulation, and as promised in its customer-facing Privacy Policy.

B. COC's Failure to Provide Reasonable, Adequate, and Compliant Data Security

18. COC clearly recognized its duty to provide reasonable data security for Plaintiffs' and Class Members' PHI/PII that it collects and stores as part of its business practices. COC's privacy policy expressly promises that "[w]e are required by law to maintain the privacy and security of your protected health information."[5]

19. COC's privacy policy further states that COC's promises to protect its patients' PHI/PII is not only a requirement under applicable law, but also "part of our code of ethics."[6] Accordingly, the privacy policy assures its patients that "we will not use or share your information other than as described here unless you tell us in writing" and that "we must follow the duties and privacy policies described in this notice."[7]

---

[4] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed January 31, 2023).

[5] "Privacy Policy" https://www.circlesofcare.org/about/privacy-policy-2/ (last accessed January 31, 2023).

[6] *Id.*

[7] *Id.*

20. Despite these promises, COC did not implement reasonable data security safeguards and protocols to protect Plaintiffs' and Class Members' PHI/PII, and ultimately allowed nefarious third-party hackers to breach their data servers and exfiltrate Plaintiffs' and Class Members' sensitive PHI/PII.

C. COC's Obligation to Protect Patient PHI/PII Under State and Federal Law

21. The duty of businesses such as COC to protect the PII and PHI that its patients entrust to it is recognized under Florida law, which states that entities such as Defendant, who acquire, maintain, store and use personal information, "shall take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171.2(2).

22. Further, as a HIPAA healthcare provider, COC holds a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiffs' and Class Members' PHI/PII.

23. Under the HIPAA Privacy Rule, COC is required to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives maintains or transmits;
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
d. Ensure compliance by their workforce.

45 C.F.R. § 164.306(a).

24. The HIPAA Privacy Rule also requires COC to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e) and to "[i]mplement 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" under 45 C.F.R. § 164.312(a)(1).

25. Further, the Federal Trade Commission Act, 45 U.S.C. § 45 prohibits COC from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission has found 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 Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

26. COC failed to comply with each of these state and federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PHI/PII.

///

///

D. Applicable Standards of Care

27. In addition to its obligations under state and federal law, COC owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. COC owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer system and networks, and the personnel responsible for them, adequately protected the PHI/PII of Plaintiffs and Class Members.

28. COC owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer system to ensure that the PHI/PII in Defendants' possession was adequately secured and protected.

29. COC owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in its possession, including adequately training its employees and others who accessed the PHI/PII in COC's possession, including adequately training its employees and others who accessed PII in its computer systems on how to adequately protect PHI/PII.

30. COC owed a duty of care to Plaintiffs and Class Members to implement processes that would detect a breach of its data security systems in a timely manner.

31. COC owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

32. COC owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PHI/PII to COC.

33. COC owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when the data breach occurred.

34. COC owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. COC received PHI/PII from Plaintiffs and Class Members with the understanding that Plaintiffs and Class Members expected their PHI/PII to be protected from disclosure. COC knew that a breach of its data systems would cause Plaintiffs and Class Members to incur damages.

E. Stolen Information Is Valuable to Hackers and Thieves

35. It is well known, and the subject of many media reports, that PHI/PII is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendant opted to maintain an insufficient and inadequate system to protect the PHI/PII of

Plaintiffs and Class Members.

36. Plaintiffs and Class Members value their PHI/PII, as in today's electronic-centric world, their PHI/PII is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

37. Legitimate organizations and criminal underground alike recognize the value of PHI/PII. That is why they aggressively seek and pay for it.

38. PHI/PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps."[8]

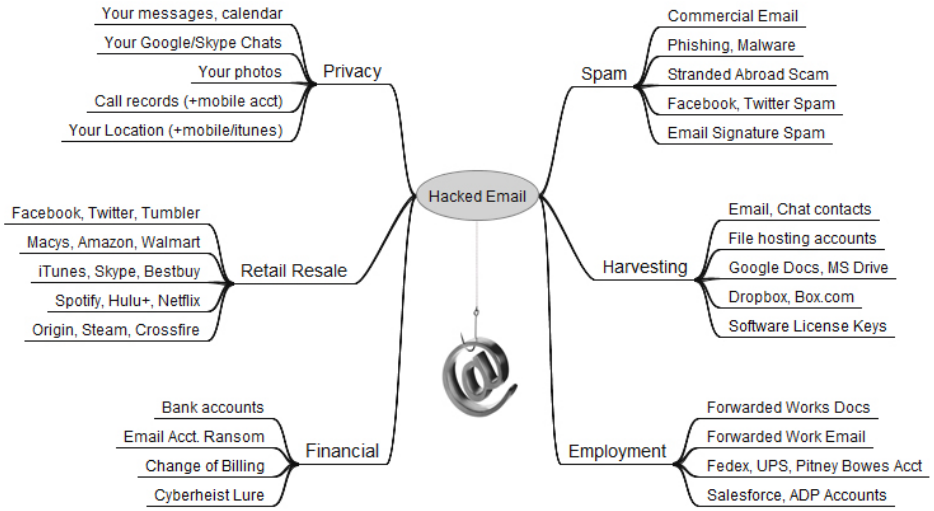
39. Once someone buys PHI/PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

40. In addition to PHI/PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also to verify accounts and reset passwords, a hacked email account

[8] *See All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/ (last accessed January 31, 2023).

could open up a number of other accounts to an attacker.[9]

41. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[10]



42. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and

---

[9] *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data. (last accessed January 31, 2023).

[10] Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/ (last accessed January 31, 2023).

credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[11]

F. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud

43. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the PHI/PII of Plaintiffs and Class Members. The ramification of Defendant's failure to keep Plaintiffs' and Class Members' data secure is severe.

44. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.[12] In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.[13] The frequency and severity of healthcare data breaches has only increased with time. 2021 was reported as the "worst ever year" for

[11] *Report on Phishing* (Oct. 2006), https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf (last accessed January 31, 2023).

[12] *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/. (last accessed January 31, 2023).

[13] *December 2019 Healthcare Data Breach*, HIPAA Journal (Jan 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed January 31, 2023).

healthcare data breaches—with at least 44,993,618 healthcare records having been exposed or stolen across 585 breaches.[14]

45. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[15] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*.

G. Annual Monetary Losses from Identity Theft Are in the Billions of Dollars

46. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

[14] "Largest Healthcare Data Breaches of 2021," HIPPA Journal (Dec. 30, 2021), https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/ (last accessed January 31, 2023)

[15] *See Victims of Identity Theft*, U.S. Department of Justice (September 2015, revised November 13, 2017), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last accessed January 31, 2023).

> data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last accessed January 31, 2023).

47. This is particularly the case with HIPAA data breaches such as Defendant's, as the information implicated, such as social security numbers or medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.[16] Victims of medical identity theft "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."[17]

48. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[18] Victims of healthcare data

---

[16] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/. (last accessed January 31, 2023).
[17] *Id.*
[18] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/. (last accessed January 31, 2023).

breaches often 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."[19]

49. Plaintiffs and 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 financial or identity fraud they suffer.

H. Plaintiffs and Class Members Suffered Damages

50. The exposure of Plaintiffs' and Class Members' PHI/PII to unauthorized third-party hackers was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. The data breach was also a result of Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PHI/PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by COC's contracts and state and federal law.

51. Plaintiffs' and Class Members' PHI/PII is private and sensitive in nature and was inadequately protected by Defendant. Defendant did not obtain

[19] *Id.*

Plaintiffs' and Class Members' consent to disclose their PHI/PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

52. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

53. Plaintiffs have also lost the value of their PHI/PII. PHI/PII is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

54. Top10VPN, a secure network provider, compiled pricing information for stolen PII, including $160.15 for online banking details, $35.00 for credit reports, and $62.61 for passports. Standalone Yahoo email accounts have been listed for as little as $0.41, while banking logins are in the range of $500, and verified Paypal accounts with high balances are listed at as much as $2,000.

55. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	$550
Auto insurance card:	$70
AAA emergency road service membership card:	$70
Wells Fargo bank statement:	$25
Wells Fargo bank statement with transactions:	$80
Rutgers State University student ID:	$70

56. Healthcare data is particularly valuable on the black market because it often contains an individual's PII and PHI, including information, such as a social security number or diagnosis and medical treatment information, that is not easily, or outright cannot be changed in response to a data breach. As a result, a healthcare data record may be valued at up to **$250 per record**.[20]

[20] "2018 Trustwave Global Security Report," TRUSTWAVE https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?rnd=131992184400000000 (last accessed January 31, 2023).

57. Defendant's wrongful actions and inactions directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PHI/PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure and theft of their PHI/PII;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PHI/PII being exposed to and misused by unauthorized third-party hackers;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PHI/PII, for which there is a well-established national and international market.

58. Finally, Plaintiffs and Class Members have lost the benefit of their bargain. Plaintiffs and Class Members entered into agreements with and provided payment to Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PHI/PII. Plaintiffs and Class Members

would not have entered into such agreements and would not have paid Defendant the amount that they paid had they known that Defendant would not reasonably and adequately protect their PHI/PII. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that that do not include reasonable and adequate data security that they actually received.

CLASS ACTION ALLEGATIONS

59. Plaintiffs bring this action on their own behalf and pursuant to the Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3), and (c)(4). Plaintiffs intend to seek certification of the following Class, initially defined as follows:

> All persons residing in the United States of America who received a data breach notice informing them that their PHI/PII had been breached by unauthorized third parties as a result of Circles of Care, Inc.'s data breach.

60. Excluded from each of the above Class is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded or

otherwise modified.

61. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Class are so numerous that the joinder of all members is impractical. Presently, Plaintiffs are aware of at least 61,170 potential Class Members. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

62. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): 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 Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PHI/PII;

b. Whether Defendant violated common and statutory law by failing to implement reasonable security procedures and practices;

c. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

d. Whether Defendant knew or should have known of the security breach prior to the disclosure;

e. Whether Defendant complied with any implied contractual obligation to use reasonable security measures;

f. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;

g. Whether Defendant knew or should have known of the security breach prior to its disclosure;

h. Whether Defendant had a duty to promptly notify Plaintiffs and Class Members that their PHI/PII was, or potentially could be, compromised;

i. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;

j. The nature of the relief, including equitable relief, to which Plaintiffs and the Class Members are entitled; and

k. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, and/or injunctive relief.

63. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PHI/PII, like that of every other Class Member, was misused and/or disclosed by Defendant.

64. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of Class Members and Plaintiffs have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Class will be fairly and adequately represented by Plaintiffs and their counsel.

65. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class Members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

66. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

67. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable

to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

Violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*

68. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 67, inclusive, of this Complaint as if set forth fully herein.

69. The Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.* provides consumers with redress if a company mishandles their electronically stored information, such as PHI/PII. The SCA was designed, in part, to protect individuals' privacy interests in personal and proprietary information.

70. Section 2702(a)(1) of the SCA states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

71. "Electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

72. Through their computer equipment, Defendants provide an "electronic communication service to the public" within the meaning of the SCA.

73. By failing to take reasonable steps to safeguard Plaintiffs' and Class Members' PHI/PII while in electronic storage, Defendants have allowed unauthorized access to its electronic systems and knowingly divulged patient PHI/PII.

74. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing or communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

75. "Remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

76. "Electronic communications system" is defined as "any wire, radio, electromagnetic, photo-optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C § 2510(14).

77. COC stores its patients' PHI/PII and utilizes such information to provide services to its patients.

78. By failing to take reasonable steps to safeguard PHI/PII and allowing its computer systems to be breached, Defendants knowingly divulged Plaintiffs' and Class Members' PHI/PII, and which allowed unauthorized persons to access and use the PHI/PII for improper purposes.

79. Upon learning that its systems had been intruded upon and information had been obtained and accessed by unauthorized third parties, Defendants failed to promptly inform Plaintiffs and Class Members of the data breach and continued to knowingly divulge PHI/PII to third parties.

80. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

COUNT II

Negligence

81. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 80, inclusive, of this Complaint as if set forth fully herein.

82. Defendant requires any individual that uses its services to provide their PII and PHI to Defendant. Defendant collects and stores this PII and PHI as a part of its regular business activities, and for its own pecuniary gain.

83. Defendant owed Plaintiffs and the Class Members a duty of care in the

handling of its patients' PHI/PII. This duty included, but was not limited to, keeping that PHI/PII secure and preventing disclosure of the PHI/PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiffs and Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PHI/PII that is entrusted to it in its ordinary course of business and transactions with customers.

84. Pursuant to Fla. Stat. § 501.171.2(2), Defendant was required to "take reasonable measures to protect and secure data in electronic form containing personal information," which included the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure."

85. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI/PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' 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, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake to satisfy their data security obligations.[21]

86. Additional industry guidelines which provide a standard of care can be found in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.[22] NIST's Framework identifies seven steps for establishing or improving a cybersecurity program (section 3.2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
>
> *Step 2: Orient*. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

[21] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last accessed January 31, 2023).

[22] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last accessed January 31, 2023).

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about

> cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.
>
> *Step 7: Implement Action Plan*. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

87. In addition to its obligations under state and federal regulations and industry standards, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in COC's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PHI/PII of Plaintiffs and Class Members.

88. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its internal data systems to ensure that the PHI/PII in Defendant's possession was adequately secured and protected.

///

89. Defendant owed a duty to Plaintiffs sand Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in its custodianship, including adequately training its employees and others who accessed PHI/PII within its computer systems on how to adequately protect PHI/PII.

90. Defendant owed a duty to Plaintiffs and Class Members to implement processes or safeguards that would detect a breach of its data security systems in a timely manner.

91. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

92. Defendant owed a duty to Plaintiffs and Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material consideration in Plaintiffs and Class Members' decisions to entrust their PHI/PII to Defendants.

93. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when data breaches occur.

94. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PHI/PII from Plaintiffs and Class Members. Defendants knew that a breach of its data systems would cause Plaintiffs and Class

Members to incur damages.

95. Defendants breached its duties of care to safeguard and protect the PHI/PII which Plaintiffs and Class Members entrusted to it. Upon information and belief, Defendant adopted inadequate safeguards to protect the PHI/PII and failed to adopt industry-wide standards set forth above in its supposed protection of the PHI/PII. Defendant failed to design, maintain, and test its computer system to ensure that the PHI/PII was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

96. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs' and Class Member's PHI/PII. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite

understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identify and address security gaps.

97. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

98. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PHI/PII, Plaintiffs and Class Members suffered damages. Plaintiffs and Class Members were damaged because their PHI/PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiffs and Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiffs and Class Members of the data breach until weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records to ensure that they do not become the victims of fraud and/or identity theft.

99. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

///

///

COUNT III

Breach of Implied Contract

100. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 99, inclusive, of this Complaint as if set forth fully herein.

101. Plaintiffs and Class Members entered into agreements for medical treatment with Defendant. In making those agreements, Defendant solicited and invited Plaintiffs and Class Members to provide their PII/PHI to Defendant as a requirement of receiving service. Plaintiffs and Class Members accepted Defendant's offers and provided their PII/PHI to enter the agreements. Inherent within those agreements was an implied contractual obligation that Defendant would implement reasonable and adequate data security to safeguard and protect the PII/PHI entrusted to Defendant by Plaintiffs and Class Members from unauthorized disclosure.

102. Thus, when Plaintiffs and Class Members provided their PII/PHI to Defendant in exchange for medical services, they entered into implied contracts with Defendant under which Defendant agreed to and was obligated to reasonably protect their PII/PHI. Plaintiffs and Class Members provided payment to Defendant, as well as their PII/PHI, under the reasonable but mistaken belief that any money they paid to Defendant in connection to its provision of medical services would be used in part

to provide reasonable and adequate data security for their PII/PHI.

103. This implied contract is acknowledged and memorialized in Defendant's customer-facing documents, including, *inter alia*, Defendant's online public-facing Privacy Policy, wherein it promises that "[w]e at Circles of Care respect your privacy. This is part of our code of ethics. We are required by law to maintain the privacy of 'protected health information (PHI) about you, to notify you of our legal duties and your legal rights, and to follow the privacy policies described in this notice."[23] Defendant's Privacy Policy goes on to assure its patients that "[w]e will not use or share your information other than as described here unless you tell us in writing" and that "[w]e must follow the duties and privacy practices described in this notice and give you a copy of it."[24]

104. Defendant did not provide reasonable and adequate data security for Plaintiffs' and Class Members' PII/PHI, and instead caused it to be disclosed to unauthorized third-party hackers. Defendant did not comply with federal statutes and regulations and did not comply with industry data security standards. In doing so, Defendant materially breached its obligations under implied contract.

105. That Defendant would implement such reasonable and adequate data security was a material prerequisite to the agreements between Plaintiffs and Class

[23] *Privacy Policy*, https://www.circlesofcare.org/about/privacy-policy-2/ (last accessed January 31, 2023).
[24] *Id.*

Members. Reasonable consumers value the privacy of their PII/PHI, and do not enter into agreements for medical services with healthcare providers that are known not to protect customer data. Accordingly, Plaintiffs and Class Members would not have entered into agreements with Defendant and would not have provided Defendant with their sensitive PII/PHI had they known that Defendant would not implement such reasonable and adequate data security.

106. As a result of Defendant's breach, Plaintiffs and Class Members have lost the benefit of their bargain. Plaintiffs and Class Members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PHI/PII and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PHI/PII. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

107. Plaintiffs and Class Members fully performed their obligations under the implied contract by providing their PHI/PII and making payments to Defendant.

108. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

COUNT IV

Quasi-Contract/Unjust Enrichment

109. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 108, inclusive, of this Complaint as if set forth fully herein.

110. Plaintiffs and Class Members provided their PII/PHI and conferred a monetary benefit upon Defendant in exchange for healthcare services. Plaintiffs and Class Members did so under the reasonable but mistaken belief that part of their monetary payment to Defendant would cover the implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII/PHI. Defendant was enriched when it sold its healthcare services at a higher price than it otherwise would have based on those reasonable but mistaken beliefs.

111. Defendant's enrichment came at the expense of Plaintiffs and Class Members, who would not have paid for Defendant's services, or would have only been willing to paid substantially less for them, had they been aware that Defendant had not implemented reasonable, adequate and statutorily mandated safeguards to protect their PII/PHI.

112. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have suffered damages in the form of their lost benefit of the bargain. Plaintiffs and Class Members entered into agreements

with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PHI/PII. Plaintiffs and Class Members would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PHI/PII. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

113. Defendant should not be permitted to retain Plaintiffs' and Class Members' lost benefits, without having adequately implemented the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards. Defendant should not be allowed to benefit at the expense of consumers who trust Defendant to protect the PII/PHI that they are required to provide to Defendant in order to receive Defendant's services.

114. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

///

///

///

COUNT V

Breach of Fiduciary Duty

115. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 114, inclusive, of this Complaint as if set forth fully herein.

116. Plaintiffs and Class Members provided their PII/PHI to Defendant in confidence and under the reasonable but mistaken belief that Defendant would protect the confidentiality of that information. Plaintiffs and Class Members would not have provided Defendant with their PII/PHI had they known that Defendant would not take reasonable and adequate steps to protect it.

117. Defendant's acceptance and storage of Plaintiffs' and Class Members' PII/PHI created a fiduciary relationship between Defendant and Plaintiffs and Class Members. As a fiduciary of Plaintiffs and Class Members, Defendant has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily complaint safeguards to protect Plaintiffs' and Class Members' PHI/PII.

118. Defendant breached its fiduciary duties to Plaintiffs and Class Members by, *inter alia,* failing to implement reasonable and adequate data security protections, failing to comply with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement reasonable and adequate data security

training for its employees, and otherwise failing to reasonably and adequately safeguard the PII/PHI of Plaintiffs and Class Members.

119. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered damages. Plaintiffs and the Class Members were damaged because their PHI/PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiffs and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiffs and Class Members of the data breach until weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records to ensure that they do not become the victims of fraud and/or identity theft.

120. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

COUNT VI

Violation of the Florida Deceptive and Unfair Trade Practices Act Fla. Stat. §§ 501.201, *et. seq.* ("FDUTPA")

121. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 120, inclusive, of this Complaint as if

set forth fully herein.

122. Plaintiffs and Class Members are "consumers" as defined under Fla. Stat. § 501.203(7).

123. Defendant advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida as defined under Fla. Stat. § 501.203(8).

124. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1). Defendant engaged in unconscionable, unfair and deceptive acts and practices by promising consumers in, *inter alia*, its Privacy Policy, that it would implement reasonable and adequate data security safeguards to protect their sensitive personal information from unauthorized disclosure, when in fact it had not implemented such safeguards.

125. Fla. Stat. § 501.204(2) states that "[i]t is the intent of the Legislature that, in construing subsection (1), due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to s.5(a)(1) of the Federal Trade Commission Act." The Federal Trade Commission has expressly found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v.*

Wyndham Worldwide Corp., 799 F.3d 236, 243 (3rd Cir. 2015).

126. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers acting reasonably under the circumstances.

127. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PHI/PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

128. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21, injunctive relief, attorneys' fees and costs, and any and all other relief

allowable by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

1. For an Order certifying the Class as defined herein and appointing Plaintiffs and their Counsel to represent the Class;
2. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PHI/PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;
3. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PHI/PII compromised.
4. For an award of damages, including actual and compensatory damages, in an amount to be determined at trial;
5. For an award of punitive and treble damages, in an amount to be determined at trial;

6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

7. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

Respectfully Submitted,

/s/ Kevin L. Lewis
Kevin L. Lewis, Esq.
Florida Bar Number: 101124

KL Law
Counsel for Plaintiff
150 South Pine Island Road, Suite 300
Plantation, Florida 33324
Telephone: (954) 551-2295
Primary Email: service@kevinlewislaw.com
Secondary Email: kl@kevinlewislaw.com

/s/ Thiago M. Coelho
Thiago M. Coelho, Esq.*
**pro hac vice forthcoming*

Wilshire Law Firm, PLC
Counsel for Plaintiff
3055 Wilshire Boulevard, 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Primary Email: thiago@wilshirelawfirm.com
Secondary Email: teamthiago@wilshirelawfirm.com

ClassAction.org
