DISTRICT COURT, EL PASO COUNTY, COLORADO 270 S. Tejon St., Colorado Springs, CO 80903 DATE FILED: December 17, 2020 4:51 PM FILING ID: 4F2E3A87B06BD CASE NUMBER: 2020CV32198 **Plaintiff:** AGNES COURSEY, on behalf of herself and on behalf of all others similarly situated, v. **Defendant:** ASPENPOINTE, INC.	▲ **COURT USE ONLY**▲
Attorneys For Plaintiff: William H. Anderson (CO Bar No. 45960) HANDLEY FARAH & ANDERSON PLLC 4730 Table Mesa Drive, Suite G-200 Boulder, CO 80305 Tel: (303) 800-9109 Fax: (844) 300-1952 wanderson@hfajustice.com *In cooperation with Finkelstein, Blankinship, Frei-Pearson and Garber, LLP and Keller Lenkner LLC* Todd S. Garber (*Pro Hac Vice* application forthcoming) FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP One North Broadway, Suite 900 White Plains, New York 10601 Tel: (914) 298-3281 Fax: (914) 824-1561 tgarber@fbfglaw.com Warren Postman (*Pro Hac Vice* application forthcoming) KELLER LENKNER LLC 1300 I Street, N.W., Suite 400E Washington, D.C. 20005 Tel: (312) 948-8463 wdp@kellerlenkner.com	Case Number: Div.: Ctrm:

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Plaintiff Agnes Coursey ("Plaintiff"), on behalf of herself and on behalf of other similarly situated individuals, by and through his undersigned attorneys, Finkelstein, Blankinship, Frei-Pearson & Garber, LLP and Keller Lenkner LLC, for her Class Action Complaint against AspenPointe, Inc. ("AspenPointe" or "Defendant") and alleges the following based on personal knowledge, the investigation of counsel, and information and belief:

NATURE OF THE ACTION

1. Plaintiff and other members of the putative class ("Class Members") are individuals whose Personally Identifiable Information ("PII") were compromised due to AspenPointe's failure to implement and maintain reasonable safeguards to protect such information.

2. The compromised PII includes Class Members' names, dates of birth, Social Security numbers, Medicaid identification numbers, diagnosis codes, admission and discharge dates, and dates of last visit -- and Protected Health Information ("PHI") -- i.e., health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services.

3. On November 19, 2020, AspenPointe issued notice (the "Notice") to its patients that it had "recently discovered unauthorized access to our network occurred between September 12, 2020 and approximately September 22, 2020. . . Based on [its] comprehensive investigation and document review, which concluded on November 10, 2020, [Defendant] discovered that [patients] full name and one or more of the following were removed from [Defendant's] network in connection with this incident: date of birth, Social Security number, Medicaid ID number, date of last visit (if any), admission date, discharge date, and/or diagnosis code."[1]

4. This class action seeks to redress AspenPointe's unlawful and negligent disclosure of approximately 295,617 individuals' PII and PHI in a massive data breach on or around September 12, 2020 ("Data Breach" or "Breach"), in violation of common law. On that date, and possibly on others, AspenPointe's inadequate security measures allowed unauthorized individuals to access the AspenPointe computer network that contained the PII and PHI of Plaintiff and other individuals.

5. For the rest of their lives, Plaintiff and the Class Members will bear an immediate and heightened risk of all manners of identity theft. Accordingly, Plaintiff brings this action as a direct and/or proximate result of the Data Breach. Plaintiff has and will continue to incur damages in the form of, *inter alia*, loss of privacy and/or the additional damages set forth in detail below.

[1] https://media.dojmt.gov/wp-content/uploads/Aspenpoint-notif.pdf

JURISDICTION AND VENUE

6. Jurisdiction and venue are proper in this Court because Defendant AspenPointe, Inc.'s principal place of business is located in Colorado Springs, Colorado.

PARTIES

7. Plaintiff Agnes Coursey is a resident of Colorado Springs, Colorado. On approximately November 19, 2020, Plaintiff -- as well as her husband and children -- received a letter from AspenPointe informing her that her PII and PHI, including "date of birth, Social Security number, Medicaid ID number, date of last visit (if any), admission date, discharge date, and/or diagnosis code" was involved in a data breach and exposed to an unauthorized third party. If Plaintiff had known that AspenPointe would not adequately protect her PII and PHI, she would not have allowed AspenPointe access to this sensitive and private information.

8. Defendant AspenPointe, Inc. is a behavioral healthcare provider with its principal place of business located at 675 Southpointe Court, Suite 100, Colorado Springs, Colorado 80906.[2] AspenPointe is a provider of behavioral health care, offering Colorado Springs counseling services, and substance abuse treatment, along with career and educational services for families and individuals.

FACTUAL BACKGROUND

I. AspenPointe Data Breach

9. Due to inadequate security precautions, at minimum between the date range September 12, 2020 to September 22, 2020, the PII and PHI of approximately 295,617 patients was exposed.

10. Individuals potentially affected by the Data Breach, including Plaintiff, were first directly notified of the breach via a letter from AspenPointe dated November 19, 2020. However, AspenPointe knew of the Data Breach in September 2020.

11. By disclosing the PII and PHI to cybercriminals, AspenPointe put all Class Members at risk of identity theft, financial fraud, and other serious harms.

12. Defendant negligently failed to take the necessary precautions required to safeguard and protect the PII and PHI of Plaintiff and the other Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

[2] https://www.aspenpointe.org/about-us; https://www.aspenpointe.org/location-contacts/administration

13. On AspenPointe's website, Defendant claims to take patient privacy very seriously and elaborates on its supposed commitment to patient privacy and confidentiality in its "Notice of Privacy Rights."[3]

14. AspenPointe also elaborates on its commitment to patient privacy in its new patient enrollment forms.[4] Defendant specifically promises its patients: "Notice of Privacy: ***Your care and the records we produce regarding that care, is protected by law. We will only speak to those individuals that you have authorized, and we will only share the information you have specified. If anyone else contacts us to ask about you, we will not provide any details regarding your care until you have authorized the individual***." (emphasis added).

15. In its new patient enrollment forms, Defendant also promises in its 'rights and responsibilities' section that: "The organization respects the needs of clients for confidentiality, privacy, and security."[5]

16. Plaintiff, her husband, and her children of ages 17 and 19 all received notice that their PII and/or PHI were compromised in the Data Breach. Plaintiff and her family are unable to afford data monitoring or other monitoring services at this time.

II. Personally Identifiable Information (PII) and Protected Health Information (PHI)

17. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

18. PII and PHI can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[6]

19. Given the nature of this breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

20. Indeed, the cybercriminals who possess Class Members' PII and PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

---

[3] https://www.aspenpointe.org/docs/default-source/default-document-library/file-20151109140336s.doc?sfvrsn=64890de6_0

[4] https://www.aspenpointe.org/docs/default-source/clinical/new-patient-paperwork---english.pdf?sfvrsn=39341de6_2

[5] *Id.*

[6] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

21. AspenPointe was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.[7]

III. Class Members Have Suffered Concrete Injury As A Result Of AspenPointe's Inadequate Security And The Data Breach It Allowed

22. Class Members reasonably expected that AspenPointe would provide adequate security protection for their PII and PHI, and correspondingly, Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

23. The cybercriminals will certainly use the Class Members' PII and PHI, and the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging credit monitoring and protection services.

24. The cybercriminals who obtained the Class Members' PII and PHI may also exploit the PII and PHI they obtained by selling the data in the so-called "dark markets." Having obtained these names, addresses, and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- applying for credit cards or spending money;
- obtaining a loan;
- filing false tax returns to secure fraudulent refunds;
- obtaining employment;
- obtaining medical care;
- stealing Social Security and other government benefits; and

[7] *See e.g.*, Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN TECH (Sept. 23, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/; Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could Be Affected*, CNN TECH (Sept. 8, 2017), https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html; Jim Finkel and David Henry, *Saks, Lord & Taylor Hit By Payment Card Data Breach*, REUTERS (Apr. 3, 2018), https://www.reuters.com/article/legal-us-hudson-s-bay-databreach/saks-lord-taylor-hit-by-payment-card-data-breach-idUSKCN1H91W7; Bill Hutchinson, *87 million Facebook Users To Find Out If Their Personal Data Was Breached*, ABC NEWS (Apr. 9, 2018), https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187.

- applying for a driver's license, birth certificate, or other public document.

25. Additionally, if a Class Member's Social Security number is used to create a false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the employee's ability to gain employment or obtain a loan.

26. As a direct and/or proximate result of AspenPointe's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII and PHI, for which there is a well-established national and international market. Moreover, health information is uniquely valuable to cybercriminals.

27. The high value of medical records on the dark web has surpassed that of Social Security and credit card numbers. These records can sell for up to $1,000 online, depending on the completeness of the information contained within, according to Experian.[8] Social Security numbers sell for $1, and credit card info goes for up to $110. But Experian reports full medical records can command up to $1,000 because they are full of all the information helpful for committing identity theft: date of birth, place of birth, credit card details, Social Security number, address, and emails.

28. Carbon Black, a cybersecurity company, reports that private health information is worth three times more than traditional personal identifying information due to the fact that health information cannot be changed like a credit card number or a password, rendering victims all the more susceptible to extortion or compromise.[9]

29. Cybercriminals are very aware of the value these healthcare records possess. These medical records contain an individual's insurance credentials, which is useful for a cybercriminal who cannot qualify or afford medical coverage and needs an expensive medical procedure.[10]

---

[8] Andrew Steger, *What Happens To Stolen Healthcare Data?*, HealthTech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon. *See also* Brian Stack, *Here's How Much Your Personal Information Is Selling For On The Dark Web*, Experian Blog (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[9] Colm Gorey, *Personal health data three times more valuable to hackers than credit card info*, siliconrepublic (June 10, 2019), https://www.siliconrepublic.com/enterprise/personal-health-data-value-cyberattacks.

[10] Nathan Eddy, *Healthcare data at big risk as hackers innovate and hone their techniques*, HealthcareITNews (Sept. 11, 2019), https://www.healthcareitnews.com/news/healthcare-data-big-risk-hackers-innovate-and-hone-their-techniques.

30. Furthermore, PII and PHI have a long shelf-life because it contains different forms of personal information, can be used in more ways than one, and it typically takes longer for an information breach to be detected.[11]

31. As the University of Illinois at Chicago Health Informatics reports: "Financial data can quickly become unusable after being stolen, because people can quickly change their credit card numbers. But medical data are not perishable, which makes them particularly valuable. Some in the medical industry speculate that medical data could grow to rival or surpass financial data in value on the black market[.]"[12]

32. Although patients can have corrected information put in their files, it is difficult to get fraudulent information removed because providers fear medical liability.

33. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[13] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[14] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[15] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. There is also a high probability that criminals who now possess Class Members' PII and PHI have not yet used the information but will do so at a later date or re-sell it.

34. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

35. Defendant's poor data security also deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its service, Plaintiff and other reasonable consumers understood and expected that they were paying for both medical services and data security, when in fact Defendant did not provide the expected data security. Accordingly,

---

[11] *Id.*

[12] *Why Data Security Is The Biggest Concern in Healthcare*, https://healthinformatics.uic.edu/blog/why-data-security-is-the-biggest-concern-of-health-care/.

[13] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.

[14] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

[15] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

IV. AspenPointe's Response To The Data Breach Is Inadequate To Protect Class Members.

36. AspenPointe has failed to provide adequate compensation to the Class Members harmed by its negligence. To date, AspenPointe has offered Class Members just one year of credit monitoring and a $1,000,000 insurance reimbursement policy -- both through IDX, an inferior service. Even if an affected individual accepts the credit monitoring service, it will not provide that individual any compensation for the costs and burdens associated with fraudulent activity resulting from the Data Breach that took place prior to signing up for the service. AspenPointe has not offered Class Members any assistance in dealing with the IRS or state tax agencies. Nor has AspenPointe offered to reimburse Class Members for any costs incurred as a result of falsely filed tax returns, a common consequence of the Data Breach.

37. The offered credit monitoring service is inadequate to protect the Class Members from the threats they face. It does nothing to protect *against* identity theft. Instead, it only provides various measures to identify identity theft once it has already been committed.

38. Defendant breached its duty of care in negligently maintaining Plaintiff's PII. A reasonable person would not have shared PII and PHI with Defendant if they had known that it would not be secure and would be negligently maintained by Defendant.

39. Defendant has a duty to protect its patrons and patrons' property.

40. Defendant should have known -- and perhaps had actual knowledge -- that data breaches and especially health data -- were on the rise and medical institutions were lucrative or likely targets of cybercriminals looking to steal PII. As mentioned above, data breaches such as the one that occurred at AspenPointe dominated headlines and should have been known to any and all medical institutions which take reasonable precaution to secure the data it maintains. Defendant owed an affirmative duty to exercise reasonable or ordinary care for the safety of the PII and PHI of its patients, especially given that a data breach was foreseeable. Defendant had reason to anticipate an assault on its computer system as a medical institution warehousing and storing valuable and private information of its patients.

41. Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII and PHI and as such, the law required Defendant to do so with ordinary or reasonable care. Defendant breached that duty when they failed to implement safety and security enough to protect from the data breach that it should have anticipated.

CLASS ACTION ALLEGATIONS

42. Pursuant to Colorado Rule of Civil Procedure (C.R.C.P.) 23, Plaintiff brings this action against AspenPointe as a class action on behalf of herself and all members of the following class of similarly situated persons (the "Class"):

> All individuals residing in Colorado whose PII and/or PHI was compromised as a result of the AspenPointe Data Breach.

43. Plaintiff reserves the right to amend the above definition(s), or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

44. Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant; any entity in which Defendant have or had a controlling interest, or which Defendant otherwise controls or controlled; and any legal representative, predecessor, successor, or assignee of Defendant.

45. This action satisfies the requirements for a class action under C.R.C.P. 23, including requirements of commonality, numerosity, and superiority.

46. Plaintiff believes that the proposed Class as described above consists of approximately 295,617 and can be identified through AspenPointe's records, though the exact number and identities of the Class Members are currently unknown to Plaintiff and her counsel. The Class is therefore so numerous that joinder of all members, whether otherwise required or permitted, is impracticable.

47. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class Members. Common questions include, but are not limited to, the following:

a. Whether and to what extent AspenPointe had a duty to protect the Class Members' PII;

b. Whether AspenPointe breached its duty to protect the Class Members' PII;

c. Whether AspenPointe disclosed Class Members' PII;

d. Whether AspenPointe timely, accurately, and adequately informed Class Members that their PII and PHI had been compromised;

e. Whether AspenPointe's conduct was negligent; and

f. Whether Plaintiff and Class Members are entitled to damages.

48. The claims asserted by Plaintiff are typical of the claims of the members of the Class she seeks to represent because, among other things, Plaintiff and Class Members sustained similar injuries as a result of Defendant's uniform wrongful conduct; Defendant owed the same duty to each Class Member; and Class Members' legal claims arise from the same conduct by Defendant.

49. Plaintiff will fairly and adequately protect the interests of the proposed Class. Plaintiff's interests do not conflict with the Class Members' interests. Plaintiff has retained class counsel experienced in class action litigation to prosecute this case on behalf of the Class.

50. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant.

51. Defendant has acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

52. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the thousands and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed Class Members to prosecute their claims individually. Trial of Plaintiff's and the Class Members' claims is manageable. Unless the Class is certified, Defendant will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

53. The prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for AspenPointe.

54. AspenPointe's wrongful actions, inaction, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiff also seeks equitable remedies for the Class.

55. AspenPointe's systemic policies and practices also make injunctive relief for the Class appropriate.

56. Absent a class action, AspenPointe will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiff and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(Negligence)

57. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

58. Plaintiff brings this claim on behalf of herself and the Class.

59. The Class Members are individuals who provided certain PII and PHI including their names, addresses, dates of birth, driver's license numbers (or other form of state- issued identification), Social Security numbers, health insurance numbers, medical record numbers, and health information related to treatment, diagnosis codes, and/or banking or financial account numbers to AspenPointe as a necessary condition of AspenPointe providing mental, behavioral, substance abuse, career, and educational services to the Class Members.

60. AspenPointe had full knowledge of the sensitivity of the PII and PHI and the types

of harm that Class Members could and would suffer if the PII and PHI were wrongfully disclosed. AspenPointe had a duty to each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Class Members were the foreseeable victims of any inadequate safety and security practices. Class Members had no ability to protect their data that was in AspenPointe's possession.

61. AspenPointe had a duty to Plaintiff and Class Members to safeguard and protect their PII. AspenPointe's duty to the Plaintiff and other Class Members included, *inter alia*, establishing processes and procedures using reasonable and industry-standard care to protect the PII and PHI from wrongful disclosure and training employees who had access to the PII and PHI as to those processes and procedures.

62. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII and PHI, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

63. Defendant had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with Class Members' PII and PHI data.

64. Defendant breached its duty of care by failing to adequately secure, safeguard, and protect the PII and PHI Class Members from theft, collection, and misuse by third parties. Defendant negligently stored and/or maintained its systems.

65. Further, Defendant, by and through its above negligent actions and/or inaction, further breached its duties to Class Members by failing to design, adopt, implement, control, manage, monitor, and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Class Members' PII and PHI within its possession, custody, and control.

66. AspenPointe admitted that Class Members' PII and PHI were wrongfully exposed as a result of the Data Breach.

67. Class Members have suffered harm as a result of Defendant's negligence, including financial injury. These victims' loss of control over the compromised PII and PHI subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from use of the compromised information.

68. It was reasonably foreseeable -- in that AspenPointe knew or should have known -- that its failure to exercise reasonable care in safeguarding and protecting Class Members' PII and PHI would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such PII and PHI or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

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

70. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Class Members' PII and PHI, the Class Members have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm -- for which they are entitled to compensation. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence and/or negligent misrepresentation.

71. Class Members are entitled to injunctive relief as well as actual damages.

SECOND CAUSE OF ACTION
(Breach of Express Contract)

72. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

73. Plaintiff brings this claim on behalf of herself, and the Class.

74. Plaintiff and Class Members entered into written agreements with AspenPointe as part of the mental, behavioral, substance abuse, career, and educational services AspenPointe provided to Class Members. The agreements involved a mutual exchange of consideration whereby AspenPointe provided these services for Class Members in exchange for payment from Class Members and / or Class Members' insurance carriers or government programs remitting payment on Class Members' behalf.

75. AspenPointe's failure to protect Class Members' PII and PHI constitutes a material breach of the terms of the agreement by AspenPointe.

76. As a direct and proximate result of AspenPointe's breach of contract with Plaintiff and Class Members, Plaintiff's children and Class Members have been irreparably harmed.

77. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully request this Court award all available damages for AspenPointe's breach of express contract.

THIRD CAUSE OF ACTION

(Breach of Implied Contract)

78. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

79. Plaintiff brings this claim on behalf of herself and the Class.

80. Class Members provided their PII and PHI to AspenPointe in order to utilize AspenPointe's mental, behavioral, substance abuse, career, and educational services.

81. Class Members provided various forms of PII and PHI to AspenPointe as a condition precedent to the employers' use of AspenPointe's services.

82. Understanding the sensitive nature of PII and PHI, AspenPointe implicitly promised Class Members that it would take adequate measures to protect their PII.

83. Indeed, a material term of this contract is a covenant by AspenPointe that it will take reasonable efforts to safeguard Class Members' PII.

84. Class Members relied upon this covenant and would not have consented to the disclosure of their PII and PHI without assurances that it would be properly safeguarded. Moreover, the covenant to adequately safeguard Class Members' PII and PHI is an implied term, to the extent it is not an express term.

85. Class Members fulfilled their obligations under the contract by providing their PII and PHI to Aspen Pointe.

86. AspenPointe, however, failed to safeguard and protect the Class Members' PII. AspenPointe's breach of its obligations under the contract between the parties directly caused Class Members to suffer injuries.

87. As the direct and proximate result of Defendant's breach of the contract between AspenPointe and the Class Members, Class Members have been and continue to be damaged as described above.

88. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully requests this Court award all relevant damages for Aspen Pointe's breach of contract.

FOURTH CAUSE OF ACTION

(Violation of the Colorado Consumer Protection Act, Colo. Rev. Stat. §6-1-101, *et seq.*)

89. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

90. Plaintiff brings this claim on behalf of herself and the Class.

91. Defendant's implied and express representations that it would adequately safeguard Class Members' PII and PHI are false and deceptive because reasonable consumers understand and expect that Defendant would provide adequate data security, and they constitute representations as to characteristics, uses, or benefits of services that such characteristics, uses, or benefits did not actually have.

92. These violations have caused financial injury to the Class Members.

93. Plaintiff and other Class Members bring this action under the Consumer Protection Act to enjoin further violations, to recover actual damages, and to recover costs of this action, including reasonable attorneys' fees.

94. The Colorado Consumer Protection Act forbids deceptive trade practices. Accepting Plaintiff and Class Members' most sensitive PII and PHI without providing adequate safeguards constitutes an unconscionable, deceptive trade practice. Because Defendant did not provide adequate data security, Plaintiff and Class Members were unable to receive a material benefit of their transactions, and the transactions were excessively one-sided.

FIFTH CAUSE OF ACTION

(Violation of Colorado's Data Security Laws, Colo. Rev. Stat. § 6-1-713.5)

95. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

96. Plaintiff brings this claim on behalf of herself and the Class.

97. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

98. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

99. Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII and PHI but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that data breaches and especially health data -- were on the rise and medical institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

100. As a result of Defendant's violation of Colo. Rev. Stat. § 6-1-716, Plaintiff and Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

101. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully request this Court award all relevant damages

SIXTH CAUSE OF ACTION

(Violation of Colorado's Security Breach Notification Laws, Colo. Rev. Stat. § 6-1-716)

102. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

103. Plaintiff brings this claim on behalf of herself and the Class.

104. Defendant's conduct violated Colo. Rev. Stat. § 6-1-716, which requires commercial entities to notify individuals within 30 days of a security that involves personal information.

105. The massive data breach occurred on or around breach September 12, 2020, however, Plaintiff and the Class Members were not notified until November 19, 2020 via letter – more than 68 days after the breach occurred.

106. Defendant unreasonably delayed informing anyone about the breach of security of Plaintiff and the Class Members' confidential and non-public information after Defendant knew the Data Breach had occurred.

107. Defendant failed to disclose to Plaintiff and Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and PHI when they knew or reasonably believed such information had been compromised.

108. As a result of Defendant's violation of Colo. Rev. Stat. § 6-1-716, Plaintiff and Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

109. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully request this Court award all relevant damages.

SEVENTH CAUSE OF ACTION

(Violation of Colo. Rev. Stat. § 27-65-121. Care and Treatment of Persons with Mental Health Disorders - Records.)

110. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

111. Plaintiff brings this claim on behalf of herself and the Class.

112. Defendant's conduct violated Colo. Rev. Stat. § 27-65-121, which requires that: "(1) Except as provided in subsection (2) of this section, all information obtained and records prepared in the course of providing any services pursuant to this article 65 to individuals pursuant to any provision of this article 65 are ***confidential and privileged matter***. . . ." (emphasis added).

113. Defendant failed to disclose to Plaintiff and Class Members, that it would be unable to safeguard their PII and PHI, in violation of state law requiring that mental and behavioral health records be strictly protected.

114. As a result of Defendant's violation of Colo. Rev. Stat. § 27-65-121, Plaintiff and Class Members receiving behavioral health treatment suffered the violation of their privileged information, the loss of privacy, and incurred personal damages.

115. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully request this Court award all relevant damages and provide injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, respectfully requests that the Court grant relief against Defendant as follows:

A. For an Order certifying that this action may be prosecuted as a class action pursuant to C.R.P.C. 23 and requiring notice thereto to be paid by Defendant;

B. Appointing Plaintiff and her counsel to represent the Class;

C. For appropriate injunctive relief and/or declaratory relief, including an Order requiring Defendant to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing its Employees' confidential information, and to provide identity theft monitoring for an additional five years;

D. Adjudging and decreeing that Defendant has engaged in the conduct alleged herein;

E. For compensatory and general damages according to proof on certain causes of action;

F. For reimbursement, restitution, and disgorgement on certain causes of action;

G. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

H. For costs of the proceedings herein;

I. For an Order awarding Plaintiff and the Class reasonable attorney's fees and expenses for the costs of this suit;

J. Trial by jury; and

K. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

Dated: December 17, 2020

Respectfully Submitted,

By: /s/ *William H. Anderson*

William H. Anderson (CO Bar No. 45960)
HANDLEY FARAH & ANDERSON PLLC
4730 Table Mesa Drive, Suite G-200
Boulder, CO 80305
Tel: (303) 800-9109
Fax: (844) 300-1952
wanderson@hfajustice.com

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
Todd. S. Garber
(*Pro Hac Vice application forthcoming*)
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 824-1561
tgarber@fbfglaw.com

KELLER LENKNER LLC
Warren Postman (*Pro Hac Vice* application forthcoming)
1300 I Street, N.W., Suite 400E
Washington, D.C. 20005
Tel: (312) 948-8463
wdp@kellerlenkner.com

Attorneys for Plaintiff and the Putative Class