Linda M. Tirelli
Tirelli Law Group LLC
50 Main Street, Suite 1265
White Plains, NY 10606
(914) 732-3222
LTirelli@TW-LawGroup.com

[Additional Counsel Appear on Signature Page]

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK
WHITE PLAINS DIVISION

----------X

Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency,

Debtor

Ch. 11 Case No. 19-23185-rdd

----------X

LANA WILK, individually and on behalf of all others similarly situated,

Plaintiff

v.

RETRIEVAL-MASTERS CREDITORS BUREAU, INC. d/b/a AMERICAN MEDICAL COLLECTION AGENCY,

Defendant.

Adv. No. 19-_____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

----------X

COMPLAINT OF PLAINTIFF LANA WILK, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, FOR DAMAGES AND INJUNCTIVE RELIEF

NOW COMES Plaintiff LANA WILK ("Plaintiff"), individually and on behalf of all others similarly situated, by her counsel Linda M. Tirelli of Tirelli Law Group LLC, and Thomas A. Zimmerman, Jr. and Matthew C. De Re of Zimmerman Law Offices, P.C., and hereby brings her Complaint against Chapter 11 Debtor Defendant RETRIEVAL-MASTERS CREDITORS BUREAU, INC. d/b/a AMERICAN MEDICAL COLLECTION AGENCY ("Defendant" or "AMCA") to the United States Bankruptcy Court and states as follows:

I. PRELIMINARY STATEMENT

1. Defendant AMCA commenced its petition for relief under Chapter 11 of Title 11 of the United States Code ("Bankruptcy Petition") on June 17, 2019. *See*, Ch. 11 Case No. 19-23185-rdd ("Bankruptcy Case"), Dkt. # 1.

2. As set forth in the *Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions* ("Fuchs Declaration") filed in the Bankruptcy Case, the Bankruptcy Petition was the ultimate result of a "cascade of events" stemming from a data breach (the "Data Breach") wherein hackers accessed and obtained data from AMCA's servers. *See*, Fuchs Declaration, Bankruptcy Case, Dkt. # 2, ¶¶ 16-21. As set forth below, the Data Breach compromised Plaintiff's and Class members' (defined below) personally identifiable information ("PII")—including their names, addresses, Social Security numbers ("SSNs"), dates of birth, personal financial information, and medical information.

3. As one of the individuals affected by the Data Breach, Plaintiff, individually, and on behalf of the Class, brings this adversary proceeding against AMCA seeking redress for the harm caused by the Data Breach.

II. PARTIES

4. Plaintiff Lana Wilk is a natural person and resident and citizen of Cook County, Illinois.

5. Defendant AMCA is a New York corporation with a principal place of business located at 4 Westchester Plaza, Suite 110, Elmsford, New York 10523.

III. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1334(b) and the General Order of Reference previously entered in this District. This is a core proceeding under 28 U.S.C. § 157(b)(2)(A) and (O).

7. This Court has supplemental jurisdiction over the state law claims asserted herein under 28 U.S.C. § 1367(a).

8. Venue is proper in this District, pursuant to 28 U.S.C. § 1391, because Defendant is a resident of this District, and a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

IV. STATEMENT OF FACTS

The Data Breach

9. AMCA is a third party collection agency which recovers the balances of patient's outstanding medical bills. According to its website, AMCA is "one of the nation's top high volume lower balance [collection] agencies managing over $1 [billion] in annual receivables."[1]

10. As a medical collection agency, AMCA is a "business associate" of "covered entities" such as "health care provider[s] who transmit[]health information in electronic form," and is thereby subject to the data security regulations and standards set forth under the Health

[1] American Medical Collection Agency, *About Us*, available at: http://amcaonline.com/about.php.

Insurance Portability and Accountability Act ("HIPAA"), the regulations implemented pursuant thereto, and other similar state and federal laws governing PII. *See, e.g.*, 45 CFR 160.103.

11. Plaintiff and Class members entrusted their PII with various healthcare providers—*i.e.*, "covered entities" as defined by 45 CFR 160.103—in order to receive medical services. Those various healthcare providers in turn shared Plaintiff's and Class members' PII with AMCA, a third party medical collection agency.

12. According to a June 6, 2019 letter AMCA sent to Plaintiff ("Plaintiff's Letter"), on March 20, 2019, AMCA "received notice of a possible security compromise of [its] web payments page from an independent third party compliance firm" and subsequently discovered that "an unauthorized user had access to [its] system between August 1, 2018 and March 30, 2019"—*i.e.*, the Data Breach. *See*, Plaintiff's Letter, attached hereto as Exhibit A; *see also*, June 3, 2019 SEC Form 8-K filed by OPKO Health Inc. ("OPKO Health Form 8-K"), p. 2, attached hereto as Exhibit B; Fuchs Declaration, ¶ 16.

13. According to Plaintiff's Letter, a regulatory filing by one of AMCA's customers, and recent news articles, Plaintiff's and Class members' PII—including their names, addresses, SSNs, dates of birth, personal financial information, and medical information—was compromised by the Data Breach. *See*, Plaintiff's Letter, Exhibit A; OPKO Health Form 8-K, p. 2, Exhibit B; CBS Baltimore, *Over 20M Patients Affected In Massive AMCA Medical Data Breach, Attorney General Frosh Warns Marylanders*, available at: https://baltimore.cbslocal.com/2019/06/12/maryland-medical-data-breach-amca.

14. However, contrary to AMCA's representations in Plaintiff's Letter and to its customers, AMCA was likely aware of the Data Brach much sooner. According to a recent news report, a cyber-security company, Gemini Advisory ("Gemini"), attempted to notify AMCA

about the Data Breach as early as March 1, 2019, but "did not get any response to phone messages [it] left" for AMCA.[2]

15. As such, AMCA knew, or should have known, about the breach as early as March 1, 2019.

16. Despite its duty to protect Plaintiff's and Class members' PII and knowledge of the Data Breach (as early as March 1, 2019 or as late as March 20, 2019), AMCA did not take immediate steps to rectify the issue, as the Data Breach continued until March 30, 2019. *See*, Plaintiff's Letter, Exhibit A; OPKO Health Form 8-K, p. 2, Exhibit B; DataBreaches.net, *American Medical Collection Agency Breach Impacted 200,000 Patients – Gemini Advisory*, May 10, 2019, available at: https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory.

17. Moreover, pursuant to 45 CFR § 164.410 and 815 ILCS 530/10, AMCA had a duty to notify Plaintiff, Class members, and/or its customers about the Data Breach "without unreasonable delay." However, AMCA did not inform Plaintiff, Class members, or its customers about the Data Breach for several months after AMCA became aware, or should have been aware, of it. *See*, Plaintiff's Letter, Exhibit A (dated June 6, 2019); OPKO Health Form 8-K, p. 2, Exhibit B (stating that AMCA informed OPKO Health of the Data Breach "around June 3, 2019"); Fuchs Declaration, ¶ 19 (stating that notice to individuals affected by the Data Breach "began to go out on Thursday, June 6, 2019"); DataBreaches.net, *American Medical Collection Agency Breach Impacted 200,000 Patients – Gemini Advisory*, May 10, 2019, available at: https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory.

[2] DataBreaches.net, *American Medical Collection Agency Breach Impacted 200,000 Patients – Gemini Advisory*, May 10, 2019, available at: https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory.

18. AMCA's failures to adopt, implement, maintain, and enforce proper data security policies and procedures resulted in Plaintiff's and other similarly situated individuals' PII being improperly disclosed to an unauthorized party.

19. In addition, after AMCA was aware, or should have been aware, of the Data Breach, AMCA did not take appropriate steps to notify Plaintiff, Class members, and/or its customers about it.

20. Accordingly, Plaintiff brings this suit on behalf of herself and a Class of similarly situated individuals against AMCA for AMCA's failure to protect their PII and take reasonable steps to remedy the Data Breach.

Damages From Data Breaches

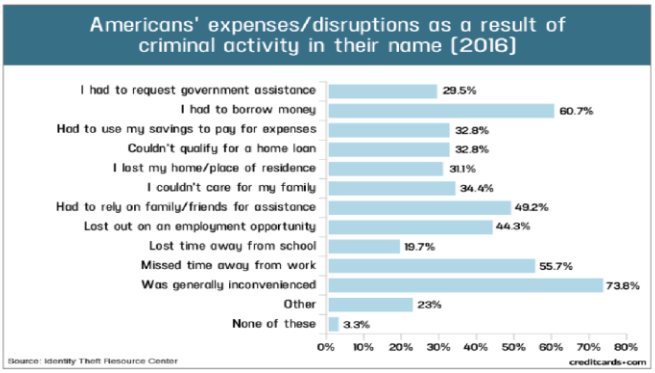
21. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[3]

22. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

23. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[3] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, p. 2, June 2007, available at: https://www.gao.gov/new.items/d07737.pdf.

24. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal information:[4]



25. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, 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 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, p. 29.

26. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. "Consumers sometimes discover their credentials have been stolen only after fraudsters use their personal medical ID to impersonate them and obtain health services. When unpaid bills are sent on to debt collectors, they track down fraud victims and seek payment."[5]

[4] Jason Steele, *Credit Card and ID Theft Statistics*, October 24, 2017, available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[5] Reuters, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, available at: https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

27. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Rush customers are at an increased risk of fraud and identity theft for years into the future.

Personal Data Protection Laws and Industry Standards

28. Title II of HIPAA contains what are known as the Administrative Simplification Provisions. *See*, 42 U.S.C. §§ 1320d, *et seq*. HIPAA requires that the Department of Health and Human Services ("Department") create rules regarding the standards for entities, such as AMCA, to follow to protect electronic personal health information from unauthorized disclosure. The Department has established regulations regarding three types of security safeguards that entities must follow for compliance: administrative, physical, and technical. For example, entities, such as AMCA, must: "(1) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required (under subpart E); and (4) ensure compliance with this subpart by its workforce." 45 CFR § 164.306(a).

29. State legislatures, such as the Illinois legislature, have also recognized the importance of safeguarding an individual's PII. For this reason, Illinois enacted the Illinois Personal Information Protection Act ("PIPA"), 815 ILCS 530/1, *et seq.*, in order to protect individuals from the harm caused by data breaches. PIPA codifies the duty of businesses to protect the personal information in the business's possession, as well as codifying the right of Illinois residents to receive prompt notification of any unauthorized access or distribution of their PII. 815 ILCS 530/10, 530/45.

30. Specifically, PIPA requires "data collectors," such as AMCA, to "implement and maintain reasonable security measures to protect [others' PII] from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45.

31. In the event of an incident of unauthorized access or disclosure of computerized data that includes PII, PIPA requires that the "data collector" notify the individual whose PII was accessed or disclosed of the data breach "immediately following discovery." 815 ILCS 530/10(b).

The Harm to Plaintiff and Class Members

32. As set forth above, AMCA failed to adopt, implement, maintain, and enforce proper data security policies and procedures in compliance with the aforementioned requirements of HIPAA, the regulations implemented pursuant thereto, and other similar state and federal laws governing individuals' PII, such as PIPA.

33. AMCA also failed to notify Plaintiff, Class members, or its customers about the Data Breach for several months after AMCA became aware of it, in violation of HIPAA, the regulations implemented pursuant thereto, and other similar state and federal laws governing individuals' PII, such as PIPA

34. As a result of AMCA's failures to comply with applicable law regarding the protection of Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was improperly disclosed to an unauthorized party.

35. Moreover, as a result of AMCA's failures to remedy the Data Breach and inform Plaintiff, Class members, and its customers of the Data Breach, a significant amount of Plaintiff's and Class members' PII was published on the "dark web" and offered for sale.[6]

[6] DataBreaches.net, *American Medical Collection Agency Breach Impacted 200,000 Patients – Gemini Advisory*, May 10, 2019, available at: https://www.databreaches.net/american-medical-collection-agency-breach-impacted-

36. As a direct and proximate result of AMCA's actions and inactions, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

37. Indeed, as a direct and proximate result of AMCA's actions and inactions, Plaintiff and members of the Class have or will suffer out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Scrutinizing credit card bills, medical bills, and bank statements for fraudulent charges;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

e. Contacting their financial institutions and closing or modifying financial accounts;

f. Resetting automatic billing and payment instructions;

g. Paying late fees and declined payment fees imposed as a result of failed automatic payments, and

h. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

38. Further, Plaintiff and Class members were harmed as a direct and proximate result of AMCA's acts and omissions described herein because Plaintiff's and Class members' property interest in their PII was compromised and their privacy was invaded. Due to these invasions of the rights, Plaintiff and the Class have suffered and will continue to suffer harms including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

200000-patients-gemini-advisory.

39. Plaintiff and the Class also incurred damages flowing from AMCA's untimely and inadequate notification of the Data Breach, as the delay in notification prevented them from taking steps earlier to protect their PII.

40. Finally, Plaintiff and the Class have an interest in ensuring that their information, which is believed to remain in the possession of AMCA, is protected from further breaches by the implementation of security measures and safeguards.

V. FACTS RELATIVE TO PLAINTIFF

41. At all times relevant, Plaintiff was a citizen of Cook County, Illinois.

42. According to Plaintiff's Letter, Plaintiff's PII was compromised in the Data Breach. *See*, Plaintiff's Letter, Exhibit A.

43. As a direct result of the Data Breach, Plaintiff took and continues to take measures that she otherwise would not have taken to ensure that her identity is not stolen and that her accounts are not compromised. For example, Plaintiff obtained and reviewed her credit report and monitored her bank account for fraudulent charges.

44. Plaintiff has suffered, and is at risk of suffering in the future, harms including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

VI. CLASS ACTION ALLEGATIONS

45. **Class Definition**: Plaintiff brings this action pursuant to Fed R. Civ. P. 23 by way of Fed. R. Bankr. P. 7023, on behalf of a nationwide class of similarly situated individuals ("the Class"), defined as follows:

All individuals whose PII was compromised in the AMCA Data Breach.

Excluded from the Class are: (1) AMCA, AMCA's agents, subsidiaries, parents, successors, predecessors, and any entity in which AMCA or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is

assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

46. **Illinois Subclass Definition**: In addition, Plaintiff brings this action pursuant to Fed R. Civ. P. 23 by way of Fed. R. Bankr. P. 7023, on behalf of a class of similarly situated individuals in Illinois ("the Illinois Subclass"), defined as follows:

> All individuals in Illinois whose PII was compromised in the AMCA Data Breach.

Excluded from the Illinois Subclass are: (1) AMCA, AMCA's agents, subsidiaries, parents, successors, predecessors, and any entity in which AMCA or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Illinois Subclass; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

47. **Numerosity and Ascertainability**: According to a recent news article, the Data Breach "affects over 20 million patients."[7] Similarly, according the Fuchs Declaration, AMCA was required to "mail well over seven million individual notices" to individuals affected by the Data Breach. *See*, Fuchs Declaration, ¶ 19. Either way, the Class is so numerous that joinder of all members is impracticable. While the exact number of Class members is presently unknown and can only be ascertained through discovery, Plaintiff believes there are millions of Class members based on the foregoing news report and the Fuchs Declaration. Class members can be identified through AMCA's records, Class members' own records, or by other means. Indeed, AMCA has likely already identified most Class members, pursuant to its obligations under 45 CFR § 164.410, as evidenced by Plaintiff's Letter and the fact that AMCA has sent notice of the

[7] CBS Baltimore, *Over 20M Patients Affected In Massive AMCA Medical Data Breach, Attorney General Frosh Warns Marylanders*, available at: https://baltimore.cbslocal.com/2019/06/12/maryland-medical-data-breach-amca.

Data Breach to over 7 million individuals. *See*, Plaintiff's Letter, Exhibit A; Fuchs Declaration, ¶ 19.

48. **Commonality and Predominance**: There are several questions of law and fact common to the claims of the Plaintiff and members of the Class, which predominate over any individual issues, including:

a. Whether AMCA adequately protected Plaintiff and Class members' PII;

b. Whether AMCA adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to its computer systems and servers;

c. Whether AMCA adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized insertion of malware on its computer systems and servers;

d. Whether AMCA properly trained its employees to prevent the unauthorized access to, and insertion of malware on, its computer systems and servers;

e. When AMCA knew or should have known about the Data Breach;

f. Whether AMCA promptly and adequately rectified the Data Breach after it became aware of the Data Breach;

g. Whether AMCA promptly notified Plaintiff, Class members, and its customers of the Data Breach;

h. Whether AMCA breached its duty to Plaintiff and Class members by its failure to adopt, implement, and maintain reasonable policies and procedures to prevent the unauthorized access to its computer systems and servers;

i. Whether AMCA owed a duty to its customers, Plaintiff and Class members to safeguard and protect the PII;

j. Whether AMCA breached its duty to its customers, Plaintiff and Class members to safeguard and protect the PII;

k. Whether AMCA breached its duty to Plaintiff and Class members by its failure to adopt, implement, and maintain reasonable policies and procedures to protect their PII;

l. Whether AMCA violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*;

m. Whether AMCA violated the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*;

n. Whether AMCA is liable for the damages suffered by Plaintiff and Class members as a result of the Data Breach.

49. **Typicality**: Plaintiff's claims are typical of the claims of the proposed Class. All claims are based on the same legal and factual issues. Plaintiff and members of the Class provided their PII to Defendant's customers, believed that their PII would be safeguarded, and had their PII compromised by the Data Breach. Defendant's conduct was uniform to Plaintiff and all Class members.

50. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. The questions of law and fact common to the proposed Class members predominate over any questions affecting only individual Class members.

51. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiff's and Class members' claims are manageable.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

52. Plaintiff repeats and realleges the allegations of paragraphs 1-51 with the same force and effect as though fully set forth herein.

53. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and the Class and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

54. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of Defendant's failure to (a) adopt, implement, and maintain reasonable security measures so that its customers' PII would not be accessed by unauthorized persons, and (b) promptly notify Plaintiff and Class members of the Data Breach.

55. Defendant also had a statutory duty to protect Plaintiff's and Class members' PII, and inform them of the Data Breach. *See, e.g.*, 45 CFR § 164.306(a); 815 ILCS 530/45. Defendant's duty also arose under section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies. Various FTC publications and data security breach orders further form the basis of Defendant's duty.

56. Plaintiff and Class members provided their PII to Defendant, through Defendant's customers, with the expectation that their PII would be safeguarded and protected. In equity and good conscience, Defendant had a duty to act in good faith and protect Plaintiff's and Class members' PII.

57. Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' PII in its possession so that the PII would not come within the possession, access, or control of unauthorized persons.

58. More specifically, Defendant's duty included, among other things, the duty to:

a. Adopt, implement, and maintain policies, procedures, and security measures for protecting PII so that unauthorized persons are not able to access it;

b. Properly train and supervise its employees and third parties to prevent the unauthorized access to PII;

c. Adopt, implement, and maintain processes to quickly detect a Data Breach and to timely act on warnings about data breaches.

59. Defendant breached its foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of its customers in its possession so that the PII would not come within the possession, access, or control of unauthorized persons.

60. Defendant also had an affirmative duty to promptly notify Plaintiff and Class members of a breach of the security of their PII if the PII was, or is reasonably believed to have been, acquired by an unauthorized person so that Plaintiff and Class members can take appropriate and timely measures to mitigate damages, protect against adverse consequences, and thwart future incidences of identity theft. *See e.g.*, 815 ILCS 530/10(b); 45 CFR § 164.410.

61. Despite the Data Breach having started on August 1, 2018, and Defendant becoming aware of it as early as March 1, 2019, Defendant did not provide notice of the Data Breach until June 2019.

62. Defendant breached its duty to promptly notify Plaintiff and Class members that their PII was accessed by unauthorized persons.

63. Through Defendant's failure to provide timely notification to Plaintiff and other Class members, Defendant prevented Plaintiff and other Class members from taking timely and

proactive steps to secure their PII and attempt to thwart the use of their PII for fraudulent purposes, including identity theft.

64. Defendant acted with reckless disregard for the security of the PII of Plaintiff and the Class because Defendant knew or should have known that its data security practices were not adequate to safeguard the PII that it collected and stored. In fact, despite being aware of the Data Breach by March 20, 2019 at the latest, Defendant did not rectify the issue until March 30, 2019.

65. Defendant acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the Data Breach so that Plaintiff and Class members could take measures to protect themselves from damages caused by the fraudulent use of the PII compromised in the Data Breach.

66. As a result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages including, but not limited to, risk of identity theft and fraudulent charges, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; and an increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

67. Plaintiff repeats and realleges the allegations of paragraphs 1-51 with the same force and effect as though fully set forth herein.

68. Plaintiff and Class members have legally protected property rights and privacy interests in their PII.

69. Defendant knew, or should have known, of Plaintiff's and Class members' legally protected interests in their PII.

70. Plaintiff and Class members provided their PII to Defendant's customers and Defendant's customers provided Plaintiff's and Class members' PII to Defendant with the expectation that the PII would be safeguarded and protected. In equity and good conscience, Defendant had a duty to act in good faith and protect Plaintiff's and Class members' PII.

71. Defendant compromised Plaintiff's and Class members' property right and invaded their privacy by failing exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of its customers in its possession so that the PII would not come within the possession, access, or control of unauthorized persons.

72. Defendant acted with reckless disregard for the security of the PII of Plaintiff and the Class because Defendant knew or should have known that its data security practices were not adequate to safeguard the PII that it collected and stored. In fact, despite being aware of the Data Breach by March 20, 2019 at the latest, Defendant did not rectify the issue until March 30, 2019.

73. As a result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages including, but not limited to, risk of identity theft and fraudulent charges, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; and an increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Violation of the Illinois Consumer Fraud and Deceptive Trade Practices Act
(815 ILCS 505/1, *et seq.*)
(On Behalf of Plaintiff and the Illinois Subclass)

74. Plaintiff repeats and realleges the allegations of paragraphs 1-51 with the same force and effect as though fully set forth herein.

75. Defendant is a "person" as defined by 815 ILCS 505/1.

76. Plaintiff and Illinois Subclass members are consumers pursuant to 815 ILCS 505/1(e).

77. Pursuant to 815 ILCS 530/20, a violation of PIPA constitutes an unlawful practice under the ICFA.

78. As a corporation that handles, collects, disseminates, and otherwise deals with nonpublic PII, Defendant is a "data collector" as defined in 815 ILCS 530/5.

79. Pursuant to 815 ILCS 530/5, "health insurance information" includes "an individual's health insurance policy number or subscriber identification number, any unique identifiers used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records" and "personal information" includes "health insurance information" and SSNs. As such, Plaintiff's and Illinois Subclass members' PII constituted both "personal information" and "health insurance information." 815 ILCS 530/5.

80. Defendant is a "data collector" that maintains or stores, but does not own or license, computerized data that includes "personal information" that the "data collector" does not own or license. 815 ILCS 530/10(b). As such, Defendant was required to notify Plaintiff and Illinois Subclass members of the Data Breach *immediately following discovery*, if the "personal

information" was, or was reasonably believed to have been, acquired by an unauthorized person. 815 ILCS 530/10(b) (emphasis added).

81. As a "data collector," Defendant was required to adopt, implement, and maintain reasonable security measures to protect Plaintiff's and Illinois Subclass members' PII from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45.

82. Defendant violated 815 ILCS 530/45 by failing to adopt, implement, and maintain reasonable security measures to protect Plaintiff's and Illinois Subclass members' PII from unauthorized access, acquisition, destruction, use, modification, or disclosure.

83. Defendant failed to notify Plaintiff and Illinois Subclass members of the Data Breach immediately following discovery, as Defendant was aware of the Data Breach as early as March 1, 2019 (and by March 20, 2019 at the latest) but did not mail notice of the Data Breach to Plaintiff and Illinois Subclass members until June 2019.

84. By failing to notify Plaintiff and Illinois Subclass members of the Data Breach immediately upon discovering it, Defendant violated 815 ILCS 530/10(b).

85. Defendant's conduct implicates consumer protection concerns as the Data Breach affects the public, including the customers of Defendant, caused Plaintiff and Illinois Subclass members to expend time and effort to place freezes or alerts with credit reporting agencies and financial institutions, obtain identity theft monitoring or protection services, and monitor and review credit reports and accounts for possible unauthorized activity that they otherwise would not have done, and will continue to cause harm to Plaintiff and Illinois Subclass members in the increased risk of identity theft, and because identity thieves may use Plaintiff's and Illinois Subclass members' PII for a variety of crimes.

86. Defendant knew or should have known that its data security measures were inadequate to safeguard Plaintiff's and other Illinois Subclass members' PII. Defendant's actions in engaging in the foregoing unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and members of the Illinois Subclass.

87. The above-described deceptive and unfair acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

88. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiff and other Illinois Subclass members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

89. As a direct and proximate result of Defendant's conduct, Plaintiff and members of the Illinois Subclass suffered damages, including but not limited to the imminent, immediate, and continued increased risk of harm of identity theft and fraud, expending time and effort to place freezes or alerts with credit reporting agencies and financial institutions, obtaining identity theft monitoring or protection services, and monitoring and reviewing credit reports and accounts for possible unauthorized activity.

90. Additionally, as a direct and proximate result of Defendant's conduct, Plaintiff and Illinois Subclass members suffered anxiety, emotional distress, and loss of privacy.

91. Plaintiff and Illinois Subclass members seek relief under 815 ILCS 505/10a for the aforementioned violations. Plaintiff and Illinois Subclass members seek damages, including,

but not limited to, actual damages, restitution, equitable relief, punitive damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Lana Wilk, individually, and on behalf of all others similarly situated, prays for an Order as follows:

A. Finding that this action satisfies the prerequisites for maintenance as a class action and certifying the Class and Illinois Subclass defined herein;

B. Designating Plaintiff as representative of the Class and Illinois Subclass, and her undersigned counsel as Class Counsel;

C. Entering judgment in favor of Plaintiff, the Class, and the Illinois Subclass, and against Defendant;

D. Awarding Plaintiff, the Class, and the Illinois Subclass actual damages and all other forms of available relief;

E. Entering an injunction requiring Defendant to adopt, implement, and maintain adequate security measures to protect Plaintiff's and Class members' PII;

F. Awarding Plaintiff, the Class, and the Illinois Subclass actual and punitive damages, attorneys' fees and costs, including interest thereon, as allowed or required by law; and

G. Granting all such further and other relief as the Court deems just and appropriate.

JURY DEMAND

Plaintiff demands a trial by jury on all counts so triable.

DATE: June 25, 2019

/s/Linda M. Tirelli
Tirelli Law Group LLC
50 Main Street, Suite 1265
White Plains, NY 10606
(914) 732-3222

Thomas A. Zimmerman, Jr.
tom@attorneyzim.com
Matthew C. De Re
matt@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
Pro Hac Vice Anticipated

Attorneys for Plaintiff, the Class, and the Illinois Subclass

Retrieval-Masters Creditors Bureau, Inc.
American Medical Collection Agency
4 Westchester Plaza, Suite 110
Elmsford, NY 10523

51 85 00027638

Personal & Confidential

June 6, 2019

LANA WILK
6659 W 79TH ST
BURBANK, IL 60459-1156

NOTICE OF DATA BREACH

Dear Lana Wilk,

We are writing to notify you about a data privacy incident involving Retrieval-Masters Creditors Bureau, Inc.(d/b/a American Medical Collection Agency) (the "company"). You are receiving this letter because we processed certain of your data in connection with a debt collection. This letter is not for collection of a debt.

What Happened?

On March 20, 2019, the company received notice of a possible security compromise of our web payments page from an independent third-party compliance firm that works with credit card companies. We have recently learned, after an external forensics review, that an unauthorized user had access to our system between August 1, 2018 and March 30, 2019, and cannot rule out the possibility that the personal information on our system was at risk during the attack.

What Information Was Involved?

The information on our system that was compromised may have included your: first and last name, name of lab or medical service provider, date of medical service, referring doctor, certain other medical information, but not test results.

What We Are Doing?

Upon receiving the March 20 notice described above, we took down our web payments page on March 22, 2019, and migrated it to a third party vendor, and retained a computer security consulting firm to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident.

What You Can Do.

Monitoring. Given the nature of the information potentially exposed, as a precautionary measure, we recommend that you remain vigilant for fraud and identity theft by reviewing and monitoring your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You are also entitled to a free credit report every twelve months from each of the agencies listed below by visiting www.annualcreditreport.com/requestReport/landingPage.action or calling the following toll free number: 1-877-322-8228. A printable, mailed version of the request form is available here: https://www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf. Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies is provided below:

Equifax	**Experian**	**TransUnion**
Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com/personal/credit-report-services	P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com/help	Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com/credit-help

Identity Theft. Contact information for the Federal Trade Commission ("FTC") is included in this letter. If you believe yo

EXHIBIT A

8-K 1 a8-kbrli6x6x19.htm 8-K

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): June 3, 2019

OPKO Health, Inc.
(Exact Name of Registrant as Specified in its Charter)

Delaware	**001-33528**	**75-2402409**
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(IRS Employer Identification No.)

4400 Biscayne Blvd. Miami, Florida	**33137**
(Address of Principal Executive Offices)	(Zip Code)

Registrant's telephone number, including area code: (305) 575-4100

Not Applicable
Former name or former address, if changed since last report

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock	OPK	NASDAQ Global Select Market

EXHIBIT B

ITEM 7.01. Regulation FD.

On or around June 3, 2019, BioReference Laboratories, Inc. ("BioReference"), a subsidiary of OPKO Health Inc. (the "Company"), was notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency ("AMCA") about unauthorized activity on AMCA's web payment page (the "AMCA Incident"). AMCA is an external collection agency that has been used in the past by BioReference and other healthcare companies. According to AMCA, the unauthorized activity occurred between August 1, 2018, and March 30, 2019. AMCA has advised BioReference that data for approximately 422,600 patients for whom BioReference performed testing was stored in the affected AMCA system. AMCA advised that AMCA's affected system includes information provided by BioReference that may have included patient name, date of birth, address, phone, date of service, provider, and balance information. In addition, the affected AMCA system also included credit card information, bank account information (but no passwords or security questions) and email addresses that were provided by the consumer to AMCA. AMCA has advised BioReference that no Social Security Numbers were compromised, and BioReference provided no laboratory results or diagnostic information to AMCA. BioReference has not been able to verify the accuracy of the information received from AMCA.

AMCA advised BioReference that it is sending notices to approximately 6,600 patients for whom BioReference performed laboratory testing and whose credit card or bank account information was stored in AMCA's affected system. AMCA indicated that it will provide these affected patients with more specific information about the AMCA Incident in addition to offering them identity protection and credit monitoring services for 24 months. AMCA has not yet provided BioReference a list of the affected patients or more specific information about them. AMCA has advised BioReference that AMCA is providing notice to state attorneys general and other state agencies as required by applicable state data breach laws.

AMCA has reported to BioReference that it is continuing to investigate this incident, has reported the AMCA Incident to law enforcement and has taken steps to increase the security of its systems, processes, and data, including shutting down its web payments page, migrating it to a third-party vendor, and hiring a cybersecurity firm to implement various safeguards to increase security. BioReference and the Company take data security very seriously, including the security of data handled by vendors. BioReference is currently seeking to obtain more information from AMCA and plans to promptly take additional steps as may be appropriate once more is known about the AMCA Incident.

BioReference has not sent any collection requests to AMCA since October 2018, and it will not send any new collection requests to AMCA. In addition, BioReference has requested that AMCA cease continuing to work on any pending collection requests involving BioReference patients.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

OPKO Health, Inc.

By: /s/ Steven D. Rubin

Date: June 6, 2019

Name: Steven D. Rubin

Title: Executive Vice President-Administration