IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

STEPHANIE FOSTER, *individually and on behalf of all others similarly situated,* Plaintiff, v. A&A SERVICES, LLC d/b/a SAV-RX, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Stephanie Foster ("Plaintiff"), by and through her undersigned counsel, hereby files this Class Action Complaint, individually and on behalf of all others similarly situated, against Defendant A&A Services, LLC d/b/a Sav-Rx ("Sav-Rx" or "Defendant"). Plaintiff bases the following allegations upon information and belief, investigation of counsel, and her own personal knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendant for its failure to properly secure and safeguard individuals' personally identifying information ("PII") and protected health information ("PHI") including, *inter alia*, individuals' names, dates of birth, Social Security numbers, email addresses, phone numbers, eligibility data, and insurance identification numbers.

2. Businesses that handle PII and PHI owe a duty to the individuals to whom that data relates. This duty to protect PII and PHI arises because it is foreseeable that its exposure to unauthorized persons—especially to hackers with nefarious intentions—will result in harm to the affected individuals.

3. The harm resulting from a data privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending

risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

4. Sav-Rx is a pharmacy benefit management ("PBM") company that provides prescription drug benefit management services for employee health plans.

5. In order to provide these services to its health plan clients, Sav-Rx is entrusted with consumer and patient PII and PHI. As Defendant is or should have been aware, these types of personal and sensitive data are highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive data may be wielded to cause significant harm to the Class Members.

6. In turn, Sav-Rx has a duty to secure, maintain, protect, and safeguard the PII and PHI with which it has been entrusted against unauthorized access and disclosure through reasonable and adequate data security measures.

7. Further, as a business associate of its client health plans under federal law, Sav-Rx knowingly obtains, collects, and stores patient PII and PHI—and has a duty to secure, maintain, protect, and safeguard the PII and PHI in its possession against unauthorized access and disclosure through reasonable and adequate data security measures. Defendant is also well-aware that PII and PHI are highly valuable to cybercriminals, making it highly foreseeable that Defendant would be the target of a cyberattack.

8. Despite Sav-Rx's duty to safeguard the PII and PHI with which it is entrusted, and the foreseeability of a data breach, Plaintiff's and Class Members' sensitive information stored in Defendant's information technology systems was accessed and acquired by unauthorized third

parties during a massive data breach that occurred on or around October 3, 2023 (the "Data Breach").[1]

9. As described herein, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals as a direct and proximate result of Defendant's failure to implement and follow basic security procedures.

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

11. Plaintiff, on behalf of herself, and the Class as defined herein, brings claims for negligence, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

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

[1] *Frequently Asked Questions & Information*, Sav-Rx, https://faq.savrx.com/ (last visited June 5, 2024).

PARTIES

13. Plaintiff Stephanie Foster is an adult who, at all relevant times, is and was a citizen of the State of Texas.

14. Defendant A&A Services, LLC d/b/a Sav-Rx is a limited liability company with its principal place of business located at 224 N Park Avenue, Fremont, Nebraska 68025. Upon information and belief, Defendant is a two-member LLC. Its members are Christy Piti and Jack Barta, who upon information and belief, are both adults who, at all relevant times, are and were citizens of the State of Nebraska. Defendant is a citizen of each state in which its members maintain citizenship. As such, Defendant is a citizen of the State Nebraska. Plaintiff will amend her Complaint should additional or alternative limited liability company members be revealed.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

16. This Court has general personal jurisdiction over Defendant, as Defendant maintains its principal place of business in Fremont, Nebraska and, at all relevant times, Defendant has engaged in substantial business activities in Nebraska, regularly conducts business in Nebraska, and has sufficient minimum contacts in Nebraska.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Defendant's principal place of business is located in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District, Defendant conducts

substantial business within this District, and Defendant has harmed Class Members residing in this District.

FACTUAL BACKGROUND

A. Defendant Collected and Stored Plaintiff's and Class Members' PII and PHI.

18. Sav-Rx is a PBM that provides prescription drug benefit management services for employee health plans.[2]

19. Sav-Rx positions itself as a "100% independent" "anti-PBM" that is "in YOUR corner." It specializes in providing pharmaceutical benefit plans for union members.[3] Since its founding over fifty years ago, it has continuously grown and now serves more than one thousand client health plans.[4]

20. Upon information and belief, while administering its services to its health plan clients, Sav-Rx receives, creates, maintains, and handles patients' PII and PHI. This information includes, *inter alia*, individuals' names, dates of birth, Social Security numbers, email addresses, phone numbers, eligibility data, and insurance identification numbers.

21. Plaintiff and Class Members directly or indirectly trusted Sav-Rx with their sensitive and confidential PII and PHI and therefore reasonably expected that Defendant would safeguard their highly sensitive PII and keep their PHI confidential.

22. Due to the sensitivity of the PII and PHI that Sav-Rx handles, it is aware of its critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

---

[2] Sav-Rx, https://savrx.com/ (last visited June 5, 2024).
[3] *Id.*
[4] *Our Story*, Sav-Rx, https://savrx.com/story/ (last visited June 5, 2024).

23. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, Sav-Rx assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

24. Despite the existence of these duties, Sav-Rx failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and PHI, and ultimately allowed nefarious third-party hackers to compromise Plaintiff's and Class Members' PII and PHI.

B. Defendant is Subject to HIPAA as a Business Associate.

25. Upon information and belief, because Sav-Rx receives, maintains, and handles PII and PHI from health care plans, Defendant qualifies as a Business Associate within the meaning of 45 C.F.R. § 160.103(3), and has entered into Business Associate Contracts or Agreements with its clients to set forth its obligations as a custodian of patient PHI.[5]

26. As a business associate, Sav-Rx is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq*.

27. Due to its status as a HIPAA-covered Business Associate, Sav-Rx is required to enter into contracts with its Covered Entities to ensure that Defendant will implement adequate safeguards to prevent unauthorized use or disclosure of patients' information, including by implementing requirements of the HIPAA Security Rule,[6] and is required to report any

[5] *See Business Associates*, U.S. Dep't. of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (denoting PBMs that manage a health plan's pharmacy network as an example of a business associate) (last visited June 6, 2024).

[6] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

unauthorized use or disclosure of PII and/or PHI, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

28. Due to the nature of Sav-Rx's business, it would be unable to engage in regular business activities without collecting and aggregating patient information that it knows and understands to be sensitive and confidential.

29. Indeed, Sav-Rx claims to process PHI pursuant to HIPAA in the Notice of Privacy Practices posted on its website.[7]

30. Despite these assurances and Sav-Rx's duty to safeguard Plaintiff's and Class Members' PII and PHI, Defendant employed inadequate data security measures to protect and secure the PII and PHI with which it was entrusted, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI stored within their computer networks.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' sensitive information, Sav-Rx assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and/or PHI from unauthorized disclosure.

32. Further, given the application of HIPAA, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Sav-Rx in order to receive pharmacy benefit services as part of their health plans, Plaintiff and Class Members reasonably expected that Sav-Rx would safeguard their highly sensitive information PII and keep their PHI confidential.

[7] *Notice of Privacy Practices*, Sav-Rx, https://savrx.com/privacy-policy-2/ (last visited June 5, 2024).

C. Defendant Knew the Risks of Storing Valuable PII and PHI.

33. Given its role in handling PII and PHI, Sav-Rx was well aware that the PII and PHI it collects and stores is highly sensitive and of significant value to those who would use it for wrongful purposes.

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

35. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem, and other healthcare partner and provider companies, including Managed Care of North America, OneTouchPoint, Inc., Shields Healthcare Group, Connexin Software, Inc., and NextGen, Inc.

36. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2023, there were 6,077 recorded data breach incidents, exposing seventeen billion records. The United States specifically saw a 19.8% increase in data breaches compared to 2022.[8]

37. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[9]

---

[8] *2024 Global Threat Intelligence Report*, Flashpoint (Feb. 29, 2024), https://go.flashpoint.io/2024-global-threat-intelligence-report-download.

[9] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited June 5, 2024).

38. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[10]

39. The healthcare industry, specifically, has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[11] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[12]

40. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[13]

41. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human

---

[10] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.
[11] *The Healthcare Industry is at Risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited June 5, 2024).
[12] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.
[13] *Id.*

Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[14]

42. As such, major, high-profile breaches have occurred in recent years at healthcare partner and provider companies including Anthem, Inc. (affecting 78.8 million individuals in 2015); American Medical Collection Agency (affecting more than twenty-six million individuals in 2019); Premera Blue Cross (affecting eleven million individuals in 2015); CareSource (affecting more than three million individuals in 2023); Excellus Health Plan, Inc. (affecting ten million individuals in 2015); and more.[15]

43. In fact, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[16] In 2023 alone, about one-third of Americans was affected by health-related data breaches.[17]

44. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

---

[14] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 5, 2024).
[15] *Healthcare Data Breach Statistics*, The HIPAA Journal (May 23, 2024), https://www.hipaajournal.com/healthcare-data-breach-statistics.
[16] Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.
[17] Ken Alltucker, *Health Care Data Breaches Hit 1 in 3 Americans Last Year: Is Your Data Vulnerable?*, USA Today (Feb. 19, 2024), https://www.usatoday.com/story/news/health/2024/02/18/health-data-breaches-hit-new-record-2023/72507651007/.

45. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

46. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[18]

47. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for

[18] *Identify Theft and Your Social Security Numbers,* Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

48. **Health Insurance Information**—"stolen personal health insurance information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid."[19]

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

50. Based on the value of Plaintiff's and Class Members' PII and PHI to cybercriminals, Sav-Rx knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. Sav-Rx failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

[19] Kate O'Flaherty, *Why cyber-Criminals Are Attacking Healthcare -- And How to Stop Them*, Forbes (Oct. 5, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/?sh=54e8ed1e7f69.

D. Defendant Breached its Duty to Protect PII and PHI.

51. On or about May 24, 2024, Sav-Rx reported that it had suffered a cyberattack, during which an unauthorized third party was able to access certain non-clinical systems and obtained files that contained individuals' health information.[20]

52. According to Sav-Rx, on October 8, 2023, it identified an interruption to the Sav-Rx computer network and began to secure its systems and investigate the interruption with the aid of third-party cybersecurity experts. More than six months later, on April 30, 2024, the investigation was finally concluded.[21]

53. Based on the investigation, Sav-Rx found that cybercriminals initially accessed its systems on or around October 3, 2024, and were able to access and exfiltrate the PII and PHI of approximately 2,812,336 individuals.[22] Sav-Rx also determined that the systems affected by the Data Breach were systems related to its medication benefits management services, which it provides to health plan customers.[23]

54. Following the Data Breach, Sav-Rx purportedly took steps to contain the incident and confirm that the data acquired was destroyed and not further disseminated. But even if Defendant took steps to ensure the data's deletion, i.e., paid the threat actors a likely ransom to ensure the stolen information's destruction, criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom

[20] *Notice of Data Breach*, Sav-Rx, template available at https://apps.web.maine.gov/online/aeviewer/ME/40/8912d568-e577-49a3-93ba-f9341533d332/18ee72c6-78ad-4df8-98db-51befdd4e3ff/document.html (last visited June 5, 2024).
[21] *Id.*
[22] *Id.*
[23] *Frequently Asked Questions & Information, supra* note 1.

payments (from Sav-Rx), or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

> Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.[24]

55. Indeed, Sav-Rx cannot reasonably maintain that the acquired data has been destroyed and will not be further disseminated. Defendant's own notice to impacted individuals advises them to remain to remain vigilant for incidents of fraud and identity theft, take further actions such as monitoring their own credit records, and notify their banks or financial institutions involved and law enforcement authorities of any suspicious activity. Recognizing the risk Plaintiff and Class Members continue to face, Sav-Rx further provided them with twenty (24) months of credit monitoring services.

56. Nearly seven months after the Data Breach occurred, on May 24, 2024, Sav-Rx reported the Data Breach to the Attorney General of Maine.[25] While the reported date of consumer notification is also listed as May 24, 2024, Sav-Rx states that all notice letters informing consumers of the Data Breach were sent within forty-eight hours of the conclusion of the investigation on April 30, 2024.

57. On or around this time, Plaintiff received a notice letter from Defendant informing her that her PII and PHI entrusted to Sav-Rx had been compromised in the Data Breach.

---

[24] Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/.
[25] A&A Services d/b/a Sav-Rx, *Data Breach Notification*, Att'y Gen. of Maine (May 24, 2024), https://apps.web.maine.gov/online/aeviewer/ME/40/8912d568-e577-49a3-93ba-f9341533d332.shtml.

58. Upon information and belief, Class Members received similar Data Breach notices from Sav-Rx informing them that their PII and PHI entrusted to Sav-Rx was compromised during the Data Breach.

59. These notice letters confirmed that, during the Data Breach, the unauthorized third parties were able to gain access to and exfiltrate individuals' PII and PHI.

60. The PII and PHI compromised in the Data Breach includes, *inter alia*, individuals' names, dates of birth, Social Security numbers, email addresses, phone numbers, eligibility data, and insurance identification numbers.

61. Upon information and belief, the Data Breach and resulting exposure of nearly three million individuals' PII and PHI is the direct and proximate result of Sav-Rx's failure to implement sufficient safety and security protocols.

E. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

62. Sav-Rx is prohibited by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

63. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

[26] *See Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited June 5, 2024).

64. In 2016, the FTC updated its publication titled "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses.[27] The guidelines recommend that business implement the following:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

65. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[28]

66. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer

[27] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, October 2016, available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 5, 2024).
[28] *See Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited June 5, 2024).

data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. Upon information and belief, Sav-Rx failed to properly implement one or more of the basic data security practices recommended by the FTC. Sav-Rx's failure to employ reasonable and appropriate data security measures to protect against unauthorized access individuals' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

68. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[29]

69. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[30] Upon information and belief, Sav-Rx failed to adhere to the NIST guidance.

70. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the healthcare sector, including implementing the following measures to defend against common cyberattacks:

a. Email protection systems and controls;

b. Endpoint protection systems;

[29] *See Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology (April 16, 2018), App'x A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[30] *Id.* at Table 2 pg. 26-43.

c. Identify all users and audit their access to data, application, systems, and endpoints;

d. Data protection and loss prevention measures;

e. IT asset management;

f. Network management;

g. Vulnerability management;

h. Security operations center & incident response; and

i. Cybersecurity oversight and governance policies, procedures, and processes.[31]

71. Upon information and belief, Sav-Rx's failure to protect massive amounts of PII and PHI is a result of their failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

72. Sav-Rx was well aware of its obligations to use reasonable measures to protect individuals' PII and PHI. Sav-Rx also knew it was a target for hackers, as discussed above. Despite understanding the risks and consequences of maintaining inadequate data security, Sav-Rx nevertheless failed to comply with its data security obligations, leading to the compromise of Plaintiff's and Class Members' PII and PHI.

F. Sav-Rx is Obligated Under HIPAA to Safeguard Patient PHI.

73. As discussed above, Sav-Rx is required by HIPAA to safeguard patient PHI.

74. As a business associate of health plans, Sav-Rx is an entity covered by HIPAA, which sets minimum federal standards for privacy and security of PHI.

[31] *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last visited May 31, 2024).

75. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

76. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media"; "[m]aintained in electronic media"; or "[t]ransmitted or maintained in any other form or medium."

77. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual"; or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

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

79. The Department of Health and Human Services Office for Civil Rights further recommends the following data security measures a covered entity such as Sav-Rx should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and

evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[32]

80. Upon information and belief, Sav-Rx failed to implement one or more of the above recommended data security measures.

81. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers or their business associates to disclose PHI to cybercriminals; nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

82. As such, Sav-Rx is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it creates, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

[32] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S Dep't. of Health & Human Services (last updated Mar. 17, 2022), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

83. Given the application of HIPAA to Sav-Rx, and that Plaintiff and Class Members directly and/or indirectly entrusted their PHI to Defendant in order to receive pharmacy services through their health plans, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

G. Plaintiff and Class Members Suffered Damages.

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

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

86. As a result of Sav-Rx's failures, Plaintiff and Class Members are also at substantial increased risk of suffering identity theft and fraud or misuse of their PHI.

87. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those

affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[33]

88. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[34]

89. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[35]

90. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[36]

91. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[37]

92. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft.

---

[33] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4 (Mar. 7, 2023), https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[34] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, Health IT Sec. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.
[35] *Id*.
[36] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[37] *Id*.

Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[38]

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

94. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

H. Plaintiff's Experience

95. Plaintiff is a member of one of Sav-Rx health plan clients. In order to receive pharmacy benefit services, Plaintiff was required to directly and/or indirectly provide and entrust her PII and PHI to Sav-Rx. In collecting and maintaining Plaintiff's PII and PHI, Sav-Rx undertook a duty to act reasonably in its handling of Plaintiff's PII and PHI. Sav-Rx, however, did not take reasonable care of Plaintiff's PII and PHI, leading to its exposure and compromise as direct result of Defendant's inadequate data security measures.

96. Plaintiff received a notification from Defendant informing her that her PII and PHI she directly and or indirectly provided to Sav-Rx was compromised in the Data Breach. The letter put the onus on Plaintiff to protect her PII and PHI by encouraging Plaintiff to remain vigilant and recommending that she review her account statements, monitor free credit reports and promptly report any fraudulent or suspicious activity.

[38] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited June 5, 2024).

97. Since the Data Breach, Plaintiff has experienced actual misuse of her PII and PHI as she was altered to suspicious activity on her bank account.

98. Plaintiff has suffered actual injury from having her PII and PHI exposed and/or stolen as a result of the Data Breach, including: (1) actual misuse of her PII; (b) damages to and diminution of the value of her PII and PHI, a form of intangible property that loses value when it falls into the hands of criminals; and (c) loss of privacy.

99. In addition, knowing that hackers accessed and likely exfiltrated her PII and PHI and this information is likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

100. As a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending and is not speculative given the highly sensitive nature of the PII and PHI compromised in the Data Breach.

CLASS ACTION ALLEGATIONS

101. Plaintiff brings this Class Action on behalf of herself and all other similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

102. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Data Breach of Sav-Rx's systems which occurred on or around October 3, 2024.

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

104. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

105. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are at least millions of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Sav-Rx's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 2,812,336 individuals.

106. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Sav-Rx had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Sav-Rx was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Sav-Rx's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Sav-Rx's wrongful conduct.

107. **Typicality:** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and Class Members each had their PII and PHI exposed and/or accessed by an unauthorized third party.

108. **Adequacy:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and has no

interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

109. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

110. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Sav-Rx's liability and the fact of damages is common to Plaintiff and each member of the Class. If Sav-Rx breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

111. **Injunctive Relief:** Sav-Rx has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

112. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Sav-Rx's books and records.

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

113. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

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

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

116. Defendant has 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 any inadequate security practices on the part of Defendant. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

117. Sav-Rx also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included its failure to adequately restrict access to its computer networks that held Plaintiff's and Class Members' PII and PHI.

118. Defendant's duty also arose from Defendant's position as the business associate of its health plan clients. Defendant holds itself out as a trusted provider of medication services, thereby assuming a duty to reasonably protect the information it obtains from its patients. Indeed, Defendant, who receives, maintains, collects, and handles PII and PHI from its health plan clients, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

119. Sav-Rx also knew or should have known of the inherent risk in collecting and storing massive amounts of PII and PHI, the importance of implementing adequate data security measures to protect that PII and PHI, and the frequency of cyberattacks such as the Data Breach in the healthcare sector.

120. Further, Sav-Rx's duty arose from various statutes requiring Defendant to implement reasonable data security measures, including but not limited to: Section 5 of the FTC Act and HIPAA. For example, Section 5 of the FTC Act required Defendant to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and the Class. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect highly sensitive data. Therefore, Defendant was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duties to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendant acted in violation of Section 5 of the FTC Act.

121. Similarly, HIPAA is a further source of Defendant's duty to Plaintiff and the Class, as HIPAA required Sav-Rx to take reasonable measures to protect Plaintiff's and the Class's sensitive data. Specifically, HIPAA required Sav-Rx to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. §

164.102, *et seq*. By failing to implement reasonable data security measures, Defendant acted in violation of HIPAA.

122. Sav-Rx is subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and Defendant and Class Members. The sources of Defendant's duty are identified above.

123. Defendant breached the duties owed to Plaintiff and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

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

125. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

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

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

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

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

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

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

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

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

127. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

128. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Sav-Rx and that was ultimately accessed or compromised in the Data Breach.

129. Plaintiff and Class Members conferred a monetary benefit upon Sav-Rx in the form of monies paid for healthcare services or other services. Sav-Rx's business model would not exist save for the need to ensure the security of Plaintiff's and Class Members' PII in order to provide pharmacy benefit management services to its health plan clients.

130. The relationship between Sav-Rx is not attenuated, as Plaintiff and Class Members had a reasonable expectation that the security of their PII and PHI would be maintained when they provided their PII and PHI to Defendant's health plan clients.

131. Sav-Rx accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Upon information and belief, this financial benefit was, in part, conferred, when Defendant was paid by clients to use Plaintiff's and Class Members' PII and PHI to provide pharmacy benefit management services to Sav-Rx's health plan clients. Defendant also benefitted from the receipt of Plaintiff's and Class Members' PII and PHI.

132. Sav-Rx also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of the PII and PHI.

133. But for Sav-Rx's willingness to commit to properly and safely collecting and maintaining the security of Plaintiff's and Class Members' PII and PHI, their sensitive information

would not have been transferred to and entrusted to Sav-Rx. Further, if Defendant had disclosed that its data security measures were inadequate, Sav-Rx would not have gained the trust of its health plan clients.

134. As a result of Sav-Rx's wrongful conduct, Plaintiff and Class Members suffered damages in an amount equal to the difference between their payments made with reasonable data security and privacy practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data security and privacy practices and procedures that they received.

135. Sav-Rx's enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiff's and Class Members' PII and PHI, while at the same time failing to securely maintain that information from unauthorized access and compromise.

136. In particular, Sav-Rx enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Sav-Rx instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

137. Sav-Rx should not be permitted to retain the money belonging to Plaintiff and Class Members. It would be unjust, inequitable, and unconscionable to retain the benefits it received and is still receiving from Plaintiff and Class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal and state laws and industry standards.

138. The benefit conferred upon, received, and enjoyed by Sav-Rx was not conferred gratuitously, and it would be inequitable and unjust for Sav-Rx to retain the benefit.

139. Plaintiff and Class Members are without an adequate remedy at law.

140. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services, or Defendant should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

141. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

142. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Class Action Complaint.

143. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her

PII and PHI and remains at imminent risk that further compromises of her PII and/or PHI will occur in the future.

144. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Defendant owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

145. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI.

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

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

148. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of

Defendant's systems, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

DEMAND FOR JURY TRIAL

Please take notice that Plaintiff demands a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

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

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

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

C. For compensatory damages on behalf of Plaintiff and the Class;

D. For punitive damages on behalf of Plaintiff and the Class;

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

F. Declaratory and injunctive relief as described herein;

G. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

H. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

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

J. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

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

Dated: June 7, 2024

Respectfully submitted,

/s/ David W. Asp
David W. Asp, MN Bar No. 344850
Karen H. Riebel, MN Bar No. 0219770*
Kate M. Baxter-Kauf, MN Bar No. 392037*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
dwasp@locklaw.com

Gary F. Lynch (PA ID No. 56887)*
Patrick D. Donathen (PA ID No. 330416)*
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
patrick@lcllp.com

**pro hac vice forthcoming*

Attorneys for Plaintiff

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

STEPHANIE FOSTER

(b) County of Residence of First Listed Plaintiff Johnson
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Lockridge Grindal Nauen, PLLP,
100 Washington Avenue South, Suite 2200
(612) 339-6900

DEFENDANTS

A&A SERVICES, LLC d/b/a SAV-RX

County of Residence of First Listed Defendant Dodge County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)(2)

Brief description of cause:
A class action filed by Plaintiff and all others similarly situated for Data Breach.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ Exceeds $5 Million

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE J. Rossiter, Jr. DOCKET NUMBER 8:24-cv-00206

DATE 06/07/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ David W. Asp

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.