

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION**

*IN RE: CAPTURERX DATA BREACH
LITIGATION*

THIS DOCUMENT RELATES TO:

ALL ACTIONS

Master File No. 5:21-cv-00523-OLG

**CONSOLIDATED CLASS ACTION
COMPLAINT**

(CONSOLIDATED WITH NO. 5:21-CV-
00536)

JURY TRIAL DEMANDED

Plaintiffs Daisy Trujillo and Mark Vereen (“Plaintiffs”), individually and on behalf of all others similarly situated (“Class Members”), bring this Consolidated Class Action Complaint against NEC Networks, LLC d/b/a CaptureRx (“CaptureRx”) and Rite Aid Hdqtrs. Corp.¹ (“Rite Aid”) (collectively, “Defendants”), and allege upon personal knowledge as to their own actions and the investigation of their counsel, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this Consolidated Class Action Complaint against Defendants for their failure to adequately secure and safeguard electronically stored, personally identifiable information (“PII”) and protected health information (“PHI”) that Defendants shared between

¹ The Complaint (Dkt. 1) included Rite Aid Corporation as a co-defendant, but the Court granted the parties’ stipulation to substitute Defendant Rite Aid Hdqtrs. Corp. on July 20, 2021 (ECF No. 16).

themselves, including, without limitation, full names, birthdates,² and prescription information.³

2. CaptureRx is a specialty pharmacy benefits manager.⁴ Its services include prescription claims processing, patient assistance program administration, and public health service 340B drug program administration. CaptureRx provides these services for pharmacies and healthcare providers across the United States, including Defendant Rite Aid.

3. Individuals entrust Defendants with an extensive amount of their PII and PHI. Defendants assert that they understand the importance of protecting such information, and that “Data privacy and security are among CaptureRx’s highest priorities.”

4. Despite that proclamation, however, on or before February 11, 2021, Defendant CaptureRx learned that an unauthorized actor breached its system and accessed and acquired electronic files containing the PII and PHI of Defendant Rite Aid’s customers, including Plaintiffs’ and Class Members’ data (the “Data Breach”). The data included, at least, Plaintiffs’ and Class Members’ names, dates of birth and prescription information.

5. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ PII and PHI, Defendants assumed legal and equitable duties to those individuals.

6. The exposed PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to

² Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

³ Health information, including diagnoses, treatment information, medical test results, and prescription information, is considered protected health information under the Health Insurance Portability and Accountability Act (“HIPAA”). *See* <https://www.cdc.gov/phlp/publications/topic/hipaa.html#one>.

⁴ Exhibit A (*Notice of Data Event to the Washington State Attorney General*, dated May 5, 2021, also available at: https://agportal-s3bucket.s3.amazonaws.com/Data_Breach/NECNetworksDBaCaptureRx.2021-05-05.pdf.)

criminals. Plaintiffs and Class Members face a present and immediate lifetime risk of identity theft, which is heightened here by the loss of their birthdates and specific medical treatment information in the form of prescription information.

7. This PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members.

8. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of their inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiffs and Class Members without adequate safeguards. Defendants' conduct amounts to negligence and violates federal and state statutes.

9. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the present and immediate risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

10. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII and PHI was safeguarded, failing to

take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized criminal third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

11. Plaintiff Daisy Trujillo is a citizen of California residing in Merced County, California.

12. Plaintiff Mark Vereen is a citizen of California residing in Anderson, California.

13. NEC Networks, LLC, d/b/a CaptureRx, is a Texas limited liability company with its principle place of business in San Antonio, Texas.

14. Rite Aid Hdqtrs. Corp. is incorporated in Delaware with its principle place of business in Camp Hill, Pennsylvania.

15. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Plaintiff is a citizen of California and therefore diverse from Defendant CaptureRx, which is headquartered in Texas, and Defendant Rite Aid, which is headquartered in Pennsylvania.

17. This Court has personal jurisdiction over Defendant CaptureRx because CaptureRx is a Texas LLC with its principal place of business within this District. On information and belief, some members of this limited liability company are also residents of Texas.

18. Defendant Rite Aid is subject to the personal jurisdiction of the Court because it does or transacts business in, has agents in, or is otherwise found in and has purposely availed itself of the privilege of doing business in Texas and in this District, and because the alleged misconduct was directed to Texas and this District, among others.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred or were intentionally directed to residents and customers in this District.

FACTUAL ALLEGATIONS

Background

20. Defendant Rite Aid contracted with Defendant CaptureRx to process claims related to Rite Aid's pharmacy business. The electronic files stored and/or shared by Defendants contained non-redacted and non-encrypted PII and PHI belonging to Plaintiff and Class Members. This sensitive and confidential PII, including, but not limited to, full names and birthdates, is static and does not change, and can be used to commit myriad identity crimes. The PHI involved—pharmacy information—is also sensitive and confidential, and is protected, private medical treatment information that divulges not only the types of pharmaceuticals Plaintiffs and Class Members were prescribed, but also the underlying mental or physical diagnoses.

21. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members

demand security to safeguard their PII and PHI.

22. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII and PHI from involuntary disclosure to third parties.

The Data Breach

23. On or about May 5, 2021, Defendants announced that they experienced the Data Breach.⁵ Defendants sent notice letters to various States' Attorneys General and to individuals impacted by the Data Breach. The Notice to Plaintiff Trujillo, for example, stated:

CaptureRx is a vendor that provides services to certain healthcare providers, including Rite Aid Corporation (together with its affiliates, 'Rite Aid'). CaptureRx is writing, on behalf of Rite Aid to notify you of a recent event at CaptureRx that may affect the privacy of some of your personal information.⁶

24. Also in the notice to impacted individuals, Defendants stated:

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its system. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization. CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your information was present in the relevant files. CaptureRx began the process of notifying Rite Aid on or around March 30, 2021 of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

...

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached "Steps You Can Take to Protect Personal Information."

⁵ See Exhibit A.

⁶ Exhibit B (Plaintiffs' Redacted *Notice of Security Incident*, dated May 5, 2021 and May 18, 2021, respectively).

Id.

25. Defendants admit that an unauthorized criminal party “accessed and acquired” electronic files that contained sensitive PII and PHI belonging to Plaintiffs and Class Members. Defendants also admit that the PII and PHI included “first name, last name, date of birth, and prescription information[.]”

26. In response to the Data Breach, Defendants claim that they are “working to implement additional safeguards and training to its employees.”⁷ However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with the states’ Attorneys General or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

27. What’s more, Defendants concede Plaintiffs and Class members now face a present and immediate risk of identity theft because their sensitive PII and PHI has been stolen (“acquired”) by criminals. In particular, Defendants warned Plaintiffs and Class Members in the Notice to “remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors.”⁸

28. Plaintiffs’ and Class Members’ non-encrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members. Because of this Data Breach, unauthorized individuals can easily access the PII and PHI of Plaintiffs and Class Members.

⁷ Exhibit A.

⁸ Exhibit B.

29. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted information it was maintaining for Plaintiffs and Class Members, causing their PII and PHI to be exposed.

Defendants Acquired, Collected and Stored Plaintiffs' and Class Members' PII and PHI.

30. Defendants acquired, collected, and stored Plaintiffs' and Class Members' PII and PHI.

31. As a condition of their relationships with Plaintiffs and Class Members, Defendants required that Plaintiffs and Class Members entrust Defendants with highly sensitive, confidential PII and PHI.

32. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

33. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

34. Defendants could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data that was no longer useful, especially outdated data.

35. Defendants' negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to businesses operating in the health industry to protect and secure sensitive data.

36. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

Defendants Failed to Comply with FTC Guidelines

37. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which 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.

38. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.⁹ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁰

39. The FTC further recommends 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

⁹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 11, 2021).

¹⁰ *Id.*

measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

42. Defendants failed to properly implement basic data security practices.

43. Defendants’ failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs’ and Class Members’ PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

44. Defendants were at all times fully aware of their obligation to protect the PII and PHI of Plaintiffs and Class Members. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Failed to Comply with Industry Standards

45. Experts studying cyber security routinely identify businesses operating in the healthcare industry as being particularly vulnerable to cyberattacks because of the value of the PII and PHI that they collect and maintain.

46. Several best practices have been identified that a minimum should be implemented by companies like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data. Defendant failed to follow these industry best practices.

47. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

48. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

49. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

Defendants Failed to Comply with HIPAA Standards of Conduct

50. HIPAA requires covered entities to protect against reasonably anticipated threats

to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.¹¹

51. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling the type of PII and related data that Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

52. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, required Defendants to provide notice of the breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”¹²

53. Based on information and belief, Defendants’ Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations. Defendants’ security failures include, but are not limited to, the following:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit in violation of 45 C.F.R. §164.306(a)(1);
- b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or

¹¹ HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?*, available at: <https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/> (last visited Aug. 10, 2021).

¹² Breach Notification Rule, U.S. Dep’t of Health & Human Services, available at: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added) (last visited Aug. 10, 2021).

software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

- c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);
- d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);
- e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);
- f. Failing to protect against any reasonably anticipated uses or disclosures of electronically PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);
- g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(4);
- h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;
- i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and
- j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance

with 45 C.F.R. §164.530(c).

Value of Personally Identifiable Information

54. It is well known that PII and PHI are invaluable commodities¹³ and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.¹⁴ Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.¹⁵ The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.¹⁶

55. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

56. Defendants were well aware that the PII and PHI they collect is highly sensitive and of significant value to those who would use it for wrongful purposes. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.¹⁷ Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII and PHI on multiple

¹³ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

¹⁴ https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Aug. 10, 2021)

¹⁵ *Id.*

¹⁶ *Id.* at p15.

¹⁷ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited Aug. 10, 2021).

underground Internet websites, commonly referred to as the dark web.

57. There is a market for Plaintiff's and Class Members PII and PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as \$363 per record according to the Infosec Institute.¹⁸

58. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

59. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

60. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."¹⁹

¹⁸ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at: <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Aug. 10, 2021)

¹⁹ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, available at: <https://khn.org/news/rise-of-identity-theft/> (last visited Aug. 10, 2021).

61. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

Cyber criminals are selling [medical] information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.²⁰

62. The ramifications of Defendants' failure to keep their customers' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

63. Further, criminals often trade stolen PII and PHI on the "cyber black market" for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

64. Defendants 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. This includes the significant costs that would be imposed on Defendants' clients as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Plaintiff Daisy Trujillo's Experience

65. From approximately 2005 to the present, Plaintiff Trujillo has been a customer of Rite Aid.

66. On or around May 5, 2021, Plaintiff Trujillo received the Notice of Security

²⁰ FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, *available at*: <http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf> (last visited Aug. 10, 2021).

Incident from CaptureRx informing her of the Data breach.

67. The Notice of Security Incident notified Plaintiff Trujillo that her first name, last name, date of birth, and prescription information may have been exposed.

68. As a result of the Data Breach, Plaintiff Trujillo spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

69. Additionally, Plaintiff Trujillo is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

70. Plaintiff Trujillo stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

71. Plaintiff Trujillo suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that she entrusted to Defendant for the purpose of obtaining her prescription medication, which was compromised in and as a result of the Data Breach.

72. Plaintiff Trujillo suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, as well as anxiety over possibly losing access to her necessary prescription medications.

73. Plaintiff Trujillo has suffered present and immediate injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her medical information, in combination with her name, being placed in the hands of

unauthorized third-parties and possibly criminals.

74. Plaintiff Trujillo has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant CaptureRx's possession, is protected and safeguarded from future breaches.

Plaintiff Mark Vereen's Experience

75. On or around May 18, 2021, Plaintiff Vereen received the Notice of Data Breach from CaptureRx informing him of the Data breach.²¹

76. The Notice of Data Breach Letter notified Plaintiff Vereen that his first name, last name, date of birth, and prescription information may have been exposed.

77. As a result of the Data Breach, Plaintiff Vereen spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

78. Plaintiff Vereen suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that he entrusted to Defendant for the purpose of obtaining his prescription medication, which was compromised in, and as a result of, the Data Breach.

79. Plaintiff Vereen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, as well as anxiety over possibly losing access to his necessary prescription medications.

80. Plaintiff Vereen has suffered present and immediate injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI,

²¹ Plaintiff Vereen was a customer of Midtown Health Center, Inc. *See* Exhibit B.

especially his medical information, in combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals.

81. Plaintiff Vereen has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant CaptureRx's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

82. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Code of Civil Procedure § 382, Civil Code § 1781, and other applicable law.

83. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All individuals residing in the United States whose PII and PHI (a) Defendants stored and/or shared in Defendant CaptureRx's electronic files and (b) was exposed to an unauthorized party as a result of the data breach announced on May 5, 2021 (the "Nationwide Class").

84. In addition to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate California subclass, defined as follows:

All individuals residing in California whose PII and PHI (a) Defendants stored and/or shared in Defendant CaptureRx's electronic files and (b) was exposed to an unauthorized party as a result of the data breach announced on May 5, 2021 (the "California Class").

85. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

86. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

87. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiffs and all members of the Classes were subjected to the same wrongful practices by Defendants, entitling them to the same relief.

88. The Classes are so numerous that individual joinder of its members is impracticable. Plaintiffs are informed and believe that there are over two million Class Members.²²

89. Common questions of law and fact exist as to members of the Classes and predominate over any questions which affect only individual members of the Classes. These common questions include, but are not limited to:

- a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiffs and Class Members;
- b. Whether Defendants had a duty not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendants had a duty not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiffs and

²² Defendant CaptureRx reported to the Maine Attorney General that 2,420,141 people were impacted by the Data Breach. *See* Exhibit C (Data Breach Notifications, *also available at*: <https://apps.web.maine.gov/online/aewiewer/ME/40/e1dda27c-3170-4c95-aa24-2cf75e898577.shtml> (last visited Aug. 10, 2021)).

Class Members;

- e. Whether and when Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;
- k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendants' wrongful conduct;
- l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and
- m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

90. Plaintiffs are members of the Classes they seek to represent and their claims and injuries are typical of the claims and injuries of the other Class Members.

91. Plaintiffs will adequately and fairly protect the interests of other Class Members. Plaintiffs have no interests adverse to the interests of absent Class Members. Plaintiffs are

represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

92. Defendants have acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

93. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
**(On Behalf of Plaintiffs and the Nationwide Class,
or alternatively, the California Class)**

94. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

95. Plaintiffs and Class Members provided and entrusted Defendants with certain PII and PHI, including but not limited to their full names, birthdates, and medical information,

including pharmaceutical prescriptions.

96. Plaintiffs and Class Members entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

97. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

98. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiffs and Class Members involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

99. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendants' possession was adequately secured and protected.

100. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations.

101. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and Class Members.

102. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members, which is

recognized by laws and regulations including but not limited to HIPAA, as well as the common law. That special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential PII and PHI, a necessary part of their relationships with Defendants.

103. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably safeguard" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c).

104. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

105. In addition, Defendants had a duty to employ reasonable security measures 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 confidential data.

106. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or Class Members.

107. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate security practices, including sharing and/or storing the PII and PHI of Plaintiffs and Class Members on its computer systems.

108. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and Class Members, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting

PII and PHI stored on Defendants' systems.

109. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and Class Members, including basic encryption techniques freely available to Defendants.

110. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

111. Defendants were in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

112. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

113. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and Class Members.

114. Defendants admitted that the PII and PHI of Plaintiffs and Class Members was wrongfully "accessed and acquired" by unauthorized actors as a result of the Data Breach.

115. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and Class Members

during the time the PII and PHI were within Defendants' possession or control.

116. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach, including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2 of the NIST Cybersecurity Framework Version 1.1.

117. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and Class Members in the face of increased risk of theft.

118. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

119. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI that was no longer required to retain pursuant to regulations.

120. Defendants, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

121. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII and PHI of Plaintiffs and Class Members would not have been compromised.

122. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The PII and PHI of Plaintiffs and

Class Members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

123. Additionally, 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, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

124. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

125. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

126. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

127. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

128. Defendants' misconduct also included their decision not to comply with HIPAA for the reporting, safekeeping and encrypted authorized disclosure of the PHI of Plaintiffs and Class Members.

129. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

130. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

131. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

132. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the

impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

133. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs 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.

134. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff Trujillo and the Nationwide Class,
or alternatively, the California Class against Defendant Rite Aid)

135. Plaintiff Trujillo and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

136. Through their course of conduct, Defendant Rite Aid, Plaintiff Trujillo, and Class Members entered into implied contracts for the Defendant Rite Aid to implement data security adequate to safeguard and protect the privacy of Plaintiff Trujillo's and Class Members' PII and PHI.

137. Defendant Rite Aid required Plaintiff Trujillo and Class Members to provide and entrust their PII and PHI, including full names, birthdates and prescription information and/or other information, as a condition of getting their prescriptions filled by Defendant Rite Aid and processed by Defendant CaptureRx.

138. Defendant Rite Aid solicited and invited Plaintiff Trujillo and Class Members to provide their PII and PHI as part of their regular business practices. Plaintiff Trujillo and Class Members accepted Defendant Rite Aid's offers and provided their PII and PHI to Defendants.

139. As a condition of being customers of Defendant Rite Aid, Plaintiff Trujillo and Class Members provided and entrusted their PII and PHI to Defendant Rite Aid. In so doing, Plaintiff Trujillo and Class Members entered into implied contracts with Defendant Rite Aid by which Defendant Rite Aid agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff Trujillo and Class Members if their data had been breached and compromised or stolen.

140. A meeting of the minds occurred when Plaintiff Trujillo and Class Members agreed to, and did, provide their PII and PHI to Defendant Rite Aid, in exchange for, amongst other things, the protection of their Private Information.

141. Plaintiff Trujillo and Class Members fully performed their obligations under the implied contracts with Defendant Rite Aid.

142. Defendant Rite Aid breached the implied contracts it made with Plaintiff Trujillo and Class Members by failing to safeguard and protect their PII and PHI by failing to provide timely and accurate notice to them that their PII and PHI was compromised as a result of the Data Breach.

143. As a direct and proximate result of Defendant Rite Aid's above-described breach of implied contract, Plaintiff Trujillo and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential

data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

144. As a direct and proximate result of Defendant Rite Aid's breach of the implied contracts, Plaintiff Trujillo and Class Members sustained damages as alleged herein.

145. Plaintiff Trujillo and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class,
or alternatively, the California Class)

146. Plaintiffs and Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

147. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

148. Defendants owed a duty to Plaintiffs and Class Members to keep their PII and PHI contained as a part thereof, confidential.

149. Defendants failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII and PHI of Plaintiffs and Class Members.

150. Defendants allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiffs and Class Members, by way of Defendants' failure to protect the PII and PHI.

151. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiffs and Class Members is highly offensive to a reasonable person.

152. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII and PHI to Defendants as part of their relationships with Defendants, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

153. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

154. Defendants acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

155. Because Defendants acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

156. As a proximate result of the above acts and omissions of Defendants, the PII and PHI of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

157. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII and PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff Trujillo and the Nationwide Class,
or alternatively, the California Class, Against Defendant Rite Aid)

158. Plaintiff Trujillo and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

159. At all times during Plaintiff Trujillo's and Class Members' interactions with Defendant Rite Aid, Defendant Rite Aid was fully aware of the confidential and sensitive nature of Plaintiff Trujillo's and Class Members' PII that was provided to Rite Aid.

160. As alleged herein and above, Defendant Rite Aid's relationship with Plaintiff Trujillo and Class Members was governed by terms and expectations that Plaintiff Trujillo's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

161. Plaintiff Trujillo and Class Members provided their PII to Defendant Rite Aid with the explicit and implicit understandings that they would protect and not permit the PII to be disseminated to any unauthorized third parties.

162. Plaintiff Trujillo and the Class Members also provided their PII to Defendant Rite Aid with the explicit and implicit understandings that they would take precautions to protect that PII from unauthorized disclosure.

163. Defendant Rite Aid voluntarily received in confidence the PII of Plaintiff Trujillo and Class Members with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

164. Due to Defendant Rite Aid's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiffs and Class Members was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

165. As a direct and proximate cause of Defendant Rite Aid's actions and/or omissions, Plaintiff Trujillo and Class Members have suffered damages.

166. But for Defendant Rite Aid's disclosure of Plaintiff Trujillo's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff Trujillo's and Class Members' PII as well as the resulting damages.

167. The injury and harm Plaintiff Trujillo and Class Members suffered was the reasonably foreseeable result of Defendant Rite Aid's unauthorized disclosure of Plaintiff Trujillo's and Class Members' PII. Defendant Rite Aid knew or should have known its methods of accepting and securing Plaintiff Trujillo's and Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff Trujillo's and Class Members' PII.

168. As a direct and proximate result of Defendant Rite Aid's breach of its confidence with Plaintiffs and Class Members, Plaintiff Trujillo and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity

how their PII and PHI is used; (iii) the compromise and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

169. As a direct and proximate result of Defendant Rite Aid's breaches of confidence, Plaintiff Trujillo 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 V
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices
(On Behalf of Plaintiffs and the California Class)

170. Plaintiffs and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

171. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or

misleading advertising that constitute acts of “unfair competition” as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

172. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PII and PHI of Plaintiffs and the California Class with knowledge that the information would not be adequately protected; and by storing the PII and PHI of Plaintiffs and the California Class in an unsecure environment in violation of California’s data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII and PHI of Plaintiffs and the California Class.

173. As a direct and proximate result of Defendants’ unlawful practices and acts, Plaintiffs and the California Class were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiffs and the California Class’s legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

174. Defendants knew or should have known that Defendants’ data security practices were inadequate to safeguard the PII and PHI of Plaintiffs and the California Class and that the risk of a data breach or theft was highly likely, especially given Defendants’ inability to adhere to basic encryption standards and data disposal methodologies. Defendants’ actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

175. Plaintiffs and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and the California Class of money or property that Defendant may have acquired by means of Defendants’ unlawful, and unfair business

practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendants' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VI
**Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Business Practices
(On Behalf of Plaintiffs and the California Class)**

176. Plaintiffs and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

177. Defendants engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein by soliciting and collecting the PII and PHI of Plaintiffs and the California Class with knowledge that the information would not be adequately protected and by storing the PII and PHI Plaintiffs and the California Class in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the California Class. They were likely to deceive the public into believing their PII and PHI was securely stored, when it was not. The harm these practices caused to Plaintiffs and the California Class outweighed their utility, if any.

178. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the PII and PHI of Plaintiffs and the California Class from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the California Class. They were likely to deceive the public into believing their PII

and PHI were securely stored, when they were not. The harm these practices caused to Plaintiffs and the California Class outweighed their utility, if any.

179. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiffs and the California Class were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiffs and the California Class' legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

180. Defendants knew or should have known that Defendants' data security practices were inadequate to safeguard the PII and PHI of Plaintiffs and the California Class and that the risk of a data breach or theft was highly likely, including Defendants' failure to properly encrypt files containing sensitive PII and PHI. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the California Class.

181. Plaintiffs and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and the California Class of money or property that the Defendants may have acquired by means of Defendants' unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VII
Violation of the Confidentiality of Medical Information Act ("CMIA"),
Cal. Civ. Code §§ 56, *et seq.*
(On Behalf of Plaintiffs and the California Class)

182. Plaintiffs and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

183. At all relevant times, Defendants were healthcare providers for the purposes of this cause of action because they had the “purpose of maintaining medical information to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual.”

184. Defendants are providers of healthcare for the purposes of this cause of action within the meaning of Civil Code § 56.06(a) and maintain medical information as defined by Civil Code § 56.05.

185. Plaintiffs and California Class Members are patients of Defendants for the purposes of this cause of action, as defined in Civil Code § 56.05(k).

186. Plaintiffs and California Class Members provided their PII and PHI to Defendant Rite Aid, who in turn gave it to its processor Defendant CaptureRx.

187. At all relevant times, Defendants collected, stored, managed, and transmitted Plaintiffs’ and California Class Members’ personal medical information.

188. Section 56.10(a) of the California Civil Code provides that “[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization.”

189. As a result of the Data Breach, Defendants misused, disclosed, and/or allowed third parties to access and view Plaintiffs’ and California Class Members’ personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq.*

190. As a further result of the Data Breach, the confidential nature of the Plaintiffs’ and California Class Members’ medical information was breached as a result of Defendant’s

negligence. Specifically, Defendants knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access, view, and use Plaintiffs' and California Class Members' PHI.

191. Defendants' misuse and/or disclosure of medical information regarding Plaintiffs and California Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

192. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and California Class Members' personal medical information was disclosed without written authorization.

193. By disclosing Plaintiffs' and California Class Members' PII and PHI without their written authorization, Defendants violated California Civil Code § 56, *et seq.*, and their legal duties to protect the confidentiality of such information.

194. Defendants also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

195. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs' and California Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiffs' and California Class Members' written authorization.

196. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CMIA, Plaintiffs and California Class Members are entitled to (i)

actual damages, (ii) nominal damages of \$1,000 per Plaintiff and California Class Member, (iii) punitive damages of up to \$3,000 per Plaintiff and California Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

COUNT VIII
Unjust Enrichment (Quasi Contract)
(On Behalf of Plaintiff Trujillo and the Nationwide Class,
or alternatively, the California Class, Against Defendant Rite Aid)

209. Plaintiff Trujillo and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

210. This count is plead in the alternative to the breach of implied contract count above.

211. Plaintiff Trujillo and Class Members conferred a monetary benefit to Defendant Rite Aid when they purchased goods and services and provided their PII and PHI to receive those goods and services.

212. Defendant Rite Aid knew that Plaintiff Trujillo and Class Members conferred a monetary benefit to Defendant Rite Aid when it accepted and retained that benefit. Defendant Rite Aid profited from this monetary benefit.

213. Defendant Rite Aid was supposed to use some of the money provided to it from Plaintiff Trujillo and Class Members to secure the PII and PHI belonging to Plaintiff Trujillo and Class Members by paying for administrative costs of data management and security, including hiring a processor that had reasonably adequate data security.

214. Defendant Rite Aid should not be permitted to retain money belonging to Plaintiff Trujillo and Class Members because Defendant Rite Aid failed to implement necessary security measures to protect the PII and PHI of Plaintiff Trujillo and Class Members.

215. Defendant Rite Aid gained access to the Plaintiff Trujillo and Class Members PII and PHI through inequitable means because Defendant Rite Aid failed to disclose that it used inadequate security measures.

216. Plaintiff Trujillo and Class Members were unaware of the inadequate security measures and would not have provided their PII or PHI to Defendant Rite Aid had they known of the inadequate security measures.

217. To the extent that this cause of action is pled in the alternative to the others, Plaintiff Trujillo and Class Members have no adequate remedy at law.

218. As a direct and proximate result of Defendant Rite Aid's conduct, Plaintiff Trujillo and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII of Plaintiff Trujillo and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff Trujillo and Class Members.

219. As a direct and proximate result of Defendant Rite Aid's conduct, Plaintiff Trujillo 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.

220. Defendant Rite Aid should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff Trujillo and Class Members, proceeds that it unjustly received from them. In the alternative, Rite Aid should be compelled to refund the amounts that Plaintiff Trujillo and Class Members overpaid for Rite Aid's goods and services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

- A. For an Order certifying the Nationwide Class and the California Class, and appointing Plaintiffs and their Counsel to represent each such Class;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations,

- industry standards, and federal, state or local laws;
- iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
 - iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and Class Members;
 - v. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;
 - vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;
 - ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;
 - x. requiring Defendants to conduct regular database scanning and securing

- checks;
- xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
 - xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
 - xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

- identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands that this matter be tried before a jury.

Date: August 13, 2021

Respectfully Submitted,

/s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

M. ANDERSON BERRY
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825

Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

RACHELE R. BYRD
MARISA C. LIVESAY
BRITTANY N. DEJONG
**WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP**
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
byrd@whafh.com
livesay@whafh.com
dejong@whafh.com

Gary M. Klinger (*pro hac vice*)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (202) 429-2290
Fax: (202) 429-2294
gklinger@masonllp.com

David Lietz (*pro hac vice forthcoming*)
DC Bar No. 430557
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Tel.: (202) 640-1160
dlietz@masonllp.com

Attorneys for Plaintiffs and the Putative Classes

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was served on all counsel of record on August 13, 2021 via CM/ECF, in accordance with the Federal Rules of Civil Procedure.

/s/ Joe Kendall

JOE KENDALL

Exhibit A



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Kevin Dolan
Office: (267) 930-4861
Fax: (267) 930-4771
Email: kdolan@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 5, 2021

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent NEC Networks, LLC d/b/a CaptureRx (“CaptureRx”) located at 219 East Houston Street, Suite 100 San Antonio, TX 78205, and are writing to notify your office of an incident that may affect the security of some personal information relating to 124,175 Washington residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. CaptureRx is providing this notice on behalf of the entities identified in *Exhibit A*, collectively referred to as the “notifying entities” in this notification.

Nature of the Data Event

CaptureRx is a specialty pharmacy benefits manager whose services include prescription claims processing, patient assistance program administration, and public health service 340B drug program administration. CaptureRx provides these services for pharmacies and healthcare providers across the United States, including for the above-referenced covered entities.

On February 11, 2021, CaptureRx became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed on February 6, 2021 without authorization. CaptureRx then immediately began a thorough review of the full contents of the subject files to determine what information was present at the time of the incident and the affected individuals and associated entities. On or around March 19, 2021, CaptureRx completed this review to confirm the full scope of affected individuals and associated entities to which the information related, and determined that the subject files contained first name, last name, date of birth, and prescription information for certain patients of healthcare providers for whom CaptureRx provides services.

After confirming the scope of affected individuals and associated covered entities, CaptureRx worked to provide notice to applicable healthcare providers. Between March 30, 2021 and April 7, 2021, CaptureRx

Office of the Washington Attorney General
May 5, 2021
Page 2

began mailing notice of the incident to these healthcare providers. Since then, CaptureRx has been working continuously with healthcare providers, including the notifying entities, to notify the impacted individuals of the incident.

Notice to Washington Residents

On or about May 5, 2021, CaptureRx began providing written notice of this incident to all affected individuals on behalf of the notifying entities, which includes 124,175 Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit B*. In addition, notice of this incident is posted to the CaptureRx website in substantially the same form as *Exhibit C*, and a press release was made available to media outlets in Washington in substantially the same form as *Exhibit D*.

Other Steps Taken and To Be Taken

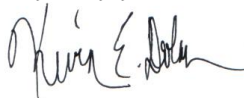
Upon discovering the event, CaptureRx moved quickly to investigate and respond to the incident, to assess the security of the information, and to notify appropriate healthcare providers of the incident, including the notifying entities. CaptureRx also notified the Federal Bureau of Investigation. CaptureRx is working with the notifying entities to notify potentially affected individuals. CaptureRx is also working to implement additional safeguards and training to its employees.

Additionally, CaptureRx is providing impacted individuals with guidance on how to protect against identity theft and fraud. CaptureRx is also providing affected individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. In addition to notifying individuals and your Office, CaptureRx will be notifying the United States Department of Health and Human Services.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4861.

Very truly yours,



Kevin Dolan of
MULLEN COUGHLIN LLC

KED/rhb

EXHIBIT A

Notifying entities

- Rite Aid – 98,964 individuals
- Skagit Valley Hospital – 21,027 individuals
- Unity Care Northwest – 4,241 individuals
- Walmart – 15,685 individuals

EXHIBIT B



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Re: Notice of Security Incident

REF 3# <<CRX ID NUMBER>>

Dear <<Name 1>>:

CaptureRx is a vendor that provides services to certain healthcare providers, including <<Entity Name Long>>. CaptureRx is writing, on behalf of <<Entity Name Short>> to notify you of a recent event at CaptureRx that may affect the privacy of some of your personal information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your information was present in the relevant files. CaptureRx began the process of notifying <<Entity Notification>> of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx’s highest priorities, and there are extensive measures in place to protect information in CaptureRx’s care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx’s systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information. As part of CaptureRx’s ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached “Steps You Can Take to Protect Personal Information.”

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,
CaptureRx

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Next of Kin of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Re: Notice of Security Incident

REF 3# <<CRX ID NUMBER>>

Dear Next of Kin of <<Name 1>>:

CaptureRx is a vendor that provides services to certain healthcare providers, including <<Entity Name Long>>. CaptureRx is writing, on behalf of <<Entity Name Short>> to notify you of a recent event at CaptureRx that may affect the privacy of some of your deceased loved one’s personal information. We are providing you with information about the event, our response to it, and resources available to you to help protect your loved one’s information, should you feel it appropriate to do so.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your loved one’s information was present in the relevant files. CaptureRx began the process of notifying <<Entity Notification>> of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your loved one’s first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx’s highest priorities, and there are extensive measures in place to protect information in CaptureRx’s care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx’s systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information. As part of CaptureRx’s ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached “Steps You Can Take to Protect Personal Information.”

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,
CaptureRx

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Accounts

To further protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your loved one's account statements, and to monitor his or her credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

Contact information for the three consumer reporting agencies is listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You can also request, in writing, that the report list the following alert:

“Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency).”

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection or <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your loved one's name and what to do if your loved one's identity becomes subject to such fraud.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts and security freezes, and the steps you can take to protect your loved one, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Parent or Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Re: Notice of Security Incident REF 3# <<CRX ID NUMBER>>

Dear Parent or Guardian of <<Name 1>>:

CaptureRx is a vendor that provides services to certain healthcare providers, including <<Entity Name Long>>. CaptureRx is writing, on behalf of <<Entity Name Short>> to notify you of a recent event at CaptureRx that may affect the privacy of some of your minor child’s personal information. We are providing you with information about the event, our response to it, and resources available to you to help protect your minor’s information, should you feel it appropriate to do so.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your minor’s information was present in the relevant files. CaptureRx began the process of notifying <<Entity Notification>> of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your minor’s first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx’s highest priorities, and there are extensive measures in place to protect information in CaptureRx’s care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx’s systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information. As part of CaptureRx’s ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached “Steps You Can Take to Protect Personal Information.”

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,
CaptureRx

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Accounts

Typically, a minor under the age of eighteen does not have credit in his or her name, and the consumer reporting agencies do not have a credit report in a minor's name. To find out if your minor has a credit report or to request a manual search for your minor's Social Security number each credit bureau has its own process. Consumers with a credit report may obtain one free report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your or your minor's credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you or your minor are a victim of identity theft, you or your minor are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a security freeze, individuals with established credit have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If the minor is a victim of identity theft, he/she is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if your minor is a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

EXHIBIT C

CaptureRx – Notice of Data Incident

May 5, 2021

CaptureRx is a vendor for certain healthcare providers and is providing notice of a recent event at CaptureRx that may affect the privacy of certain data CaptureRx received from these healthcare providers. This notification provides information about the event, CaptureRx's response to it, and resources available to individuals to help protect their information, should they feel it necessary to do so. CaptureRx is providing this notice on behalf of multiple healthcare providers, and a full list can be found here.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx then immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx completed this review to confirm the full scope of affected individuals and associated covered entities to which the information related. Between March 30, 2021 and April 7, 2021 CaptureRx began the process of notifying healthcare providers of this incident. Since then, CaptureRx has worked with healthcare providers to notify the affected individuals whose information was identified by the review.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained first name, last name, date of birth, and prescription information.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx's highest priorities, and there are extensive measures in place to protect information in CaptureRx's care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx's systems, reviewing the contents of the relevant files for sensitive information, and notifying covered entities associated with that sensitive information. As part of CaptureRx's ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event. CaptureRx is also working with healthcare providers to notify individuals whose information was contained in the subject files as well as notifying appropriate regulatory authorities.

What You Can Do. CaptureRx encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Additional steps individuals can take is provided in the below "Steps You Can Take to Protect Personal Information."

For More Information. CaptureRx has established a dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time for any questions individuals have.

Steps You Can Take To Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

EXHIBIT D

CaptureRx – Notice of Data Incident

San Antonio, TX (May 5, 2021) - CaptureRx is a vendor for certain healthcare providers and is providing notice of a recent event at CaptureRx that may affect the privacy of certain data CaptureRx received from these healthcare providers. This notification provides information about the event, CaptureRx's response to it, and resources available to individuals to help protect their information, should they feel it necessary to do so.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx then immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx completed this review to confirm the full scope of affected individuals and associated covered entities to which the information related. Between March 30, 2021 and April 7, 2021 CaptureRx began the process of notifying healthcare providers of this incident. Since then, CaptureRx has worked with healthcare providers to notify the affected individuals whose information was identified by the review.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained first name, last name, date of birth, and prescription information.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx's highest priorities, and there are extensive measures in place to protect information in CaptureRx's care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx's systems, reviewing the contents of the relevant files for sensitive information, and notifying covered entities associated with that sensitive information. As part of CaptureRx's ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event. CaptureRx is also working with healthcare providers to notify individuals whose information was contained in the subject files as well as appropriate regulatory authorities.

What You Can Do. CaptureRx encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Additional steps individuals can take is provided in the below "Steps You Can Take to Protect Personal Information."

For More Information. CaptureRx has established a dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time for any questions individuals have.

Steps You Can Take To Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

Exhibit B



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336



400492950002353780
DAISY TRUJILLO

May 5, 2021

Re: Notice of Security Incident

REF [REDACTED]

Dear Daisy Trujillo:

CaptureRx is a vendor that provides services to certain healthcare providers, including Rite Aid Corporation (together with its affiliates, 'Rite Aid'). CaptureRx is writing, on behalf of Rite Aid to notify you of a recent event at CaptureRx that may affect the privacy of some of your personal information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your information was present in the relevant files. CaptureRx began the process of notifying Rite Aid on or around March 30, 2021 of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx's highest priorities, and there are extensive measures in place to protect information in CaptureRx's care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx's systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information. As part of CaptureRx's ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached "Steps You Can Take to Protect Personal Information."

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,
CaptureRx

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336



400492950018705726
000 0004024 00000000 0001 0001 04024 INS: 0 0

MARK VEREEN

ANDERSON CA

May 18, 2021

Re: Notice of Security Incident

REF 3# 7TI67

Dear Mark Vereen:

CaptureRx is a vendor that provides services to certain healthcare providers, including Midtown Health Center, Inc.. CaptureRx is writing, on behalf of Midtown Health Center, Inc. to notify you of a recent event at CaptureRx that may affect the privacy of some of your personal information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your information was present in the relevant files. CaptureRx began the process of notifying Midtown Health Center, Inc. on or around March 30, 2021 of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx's highest priorities, and there are extensive measures in place to protect information in CaptureRx's care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx's systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information. As part of CaptureRx's ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached "Steps You Can Take to Protect Personal Information."

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (855) 654-0919 (toll free), Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,
CaptureRx



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

Exhibit C

Office of the Maine Attorney General

[Home](#) > [Consumer Information](#) > [Privacy, Identity Theft and Data Security Breaches](#) > [Data Breach Notifications](#)

Data Breach Notifications

Entity Information

- Type of Organization: **Healthcare**
- Entity Name: **NEC Networks, LLC d/b/a CaptureRx**
- Street Address: **219 East Houston Street, Suite 100**
- City: **San Antonio**
- State, or Country if outside the US: **Texas**
- Zip Code: **78205**

Submitted By

- Name: **Stacey Alderink**
- Title: **Director of Compliance**
- Firm name (if different than entity):
- Telephone Number: **210-587-3486**
- Email Address: **Stacey.alderink@capturerox.com**
- Relationship to entity whose information was compromised: **Employee**

Breach Information

- Total number of persons affected (including residents): **1,919,938**
- Total number of Maine residents affected: **3,215**
- If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified:
- Date(s) Breach Occured: **February 6, 2021**
- Date Breach Discovered: **March 30, 2021**
- Description of the Breach:
 - **External system breach (hacking)**
- Information Acquired - Name or other personal identifier in combination with:

Notification and Protection Services

- Type of Notification: **Written**
- Date(s) of consumer notification: **May 18, 2021**
- Copy of notice to affected Maine residents: **[CaptureRx - Wave 2 - ME - Exhibit 1 - Initial Notice.pdf](#)**
- Date of any previous (within 12 months) breach notifications: **May 5, 2021 (same incident)**
- Were identity theft protection services offered: **No**

- If yes, please provide the duration, the provider of the service and a brief description of the service:

Credits

Copyright © 2014
All rights reserved.