IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CORINA ALVARADO; ELIZABETH APPLETON; ABOLANLE ABIKOYE; BROOKE BAILEY; SHAWNA KERR, Individually and on behalf of her minor child J.K.; DAMON Miller; CARTER BUNDY, Individually and on behalf of his minor child A.B.; ROSA AKHRAS; SRINKANTH ALTURI; SCOTT PHILLIPS, Individually on behalf of his minor child H.P.; COREY BENN; and BELLVINIA BRICKLE, et. al, Plaintiffs, v. NextGen Healthcare Inc., Defendant.	Case No. 1:23-cv-02043-TWT **JURY TRIAL DEMANDED** **CLASS ACTION COMPLAINT**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs identified below (collectively "Plaintiffs"), individually and on behalf of the classes defined below of similarly situated persons, allege the following against Defendant NextGen Healthcare Inc., ("Defendant" or "NextGen"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public

documents as to all other matters.

NATURE OF THE CASE

1. NextGen, a company in the business of providing Electronic Health Record ("EHR") services to healthcare providers across the country, instituted and maintained inadequate data security measures to protect its computer systems and the sensitive information it collected and stored from unauthorized access, compromise, and exfiltration. As a provider of an EHR system, NextGen understood it had the duty and responsibility to protect patients' information that it collected, stored, and maintained, expressly advertising to potential clients that its products enable healthcare providers to "[s]ecurely exchange health information."[1] But NextGen failed to meet its duty and, as a direct result, the sensitive patient information with which it was entrusted was compromised and stolen.

2. On April 28, 2023, NextGen began notifying state attorneys general and patients that it had sustained a massive data breach in which a hacker gained unauthorized access to its EHR system (the NextGen Office system) between at least March 29, 2023, and April 14, 2023 (the "Data Breach").

---

[1] https://www.nextgen.com/services/managed-cloud (last visited May 4, 2023).

3. The hacker accessed and exfiltrated highly sensitive personally identifying information stored on the NextGen Office system, including the names, dates of birth, Social Security numbers, and/or addresses (collectively "Private Information") of more than one million patients.

4. The Data Breach occurred and was exacerbated because NextGen maintained inadequate data security procedures and practices to secure its NextGen Office system, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

5. As a healthcare technology company that provides the healthcare industry with EHR and practice management systems, NextGen is entrusted with sensitive patient information and therefore has a resulting duty to securely maintain such information in confidence and to act reasonably and implement adequate data security measures in order to protect such information against unauthorized access and disclosure.

6. NextGen is well-aware of the foreseeable risks of implementing inadequate data security measures, recognizing that "Data security threats" are among the "five tactical and strategic technology challenges that confront medical practices" and further warning that "the risk in medicine is even greater, as healthcare practices are responsible for the personal health information (PHI) of their

patients. PHI is more valuable than credit card or banking data and, therefore, a common target."[2]

7. Indeed, in the past few years, some of the largest data breaches in the healthcare industry have occurred at third-party vendors servicing the healthcare industry, such as NextGen.

8. The ramifications of NextGen's failure to adequately protect patients' Private Information are long lasting and severe. Armed with the Private Information compromised in the Data Breach, cybercriminals can and have committed a variety of crimes, including, by way of example: opening new financial accounts in Class Members' names (including a financial account in Plaintiff Alturi's name); committing financial theft (including draining Plaintiff Akhras bank account of money); taking out loans in Class Members' names; using Class Members' information to obtain government benefits; and using the Class Members' Private Information to target them with phishing and other hacking intrusions.

9. As a result of the NextGen's failure to implement adequate data security measures, Plaintiffs and Class Members have now been exposed to a present injury

[2]https://nextgen.widen.net/s/hzvtz9nzzk/ne_121019_mcs_datasecurity_whitepaper_lowres (last visited Oct. 16, 2023).

in the form of actual misuse of their Private Information and have further been exposed to a certainly impending, substantial, heightened, and imminent risk of financial fraud and identity theft for years to come. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts, credit reports, and tax returns to secure their accounts in an effort to deter and detect identity theft and fraud.

10. Plaintiffs and Class Members have and will continue to suffer injury from incurring out-of-pocket costs for, by way of example, purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft and fraud because the exposed information includes Social Security numbers and other immutable personal details.

11. Through this Consolidated Class Action Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all others similarly situated whose Private Information was compromised during the Data Breach.

PARTIES

12. Defendant NextGen Healthcare Inc. is a Delaware corporation registered with the state of Georgia as a Foreign Profit Corporation with its principal place of business at 3525 Piedmont Rd., NE, Building 6, Suite 700, Atlanta, Georgia 30305.

13. Plaintiff **Corina Alvarado** is and at all relevant times was a citizen of the State of California and the United States. Alvarado is a resident of the State of California and intends to remain domiciled in California.

14. Plaintiff **Elizabeth Appleton** is and at all relevant times was a citizen of the State of California and the United States. Appleton is a resident of the State of California and intends to remain domiciled in California.

15. Plaintiff **Abolanle Abikoye** is and at all relevant times was a citizen of the State of Georgia and the United States. Abikoye is a resident of the State of Georgia and intends to remain domiciled in Georgia.

16. Plaintiff **Brooke Bailey** is and at all relevant times was a citizen of the State of Illinois and the United States. Bailey is a resident of the State of Illinois and intends to remain domiciled in Illinois.

17. Plaintiff **Shawna Kerr** is the next friend and natural parent of her minor son J.K. They are and at all relevant times were citizens of the State of Iowa and the United States. They are residents of the State of Iowa and intend to remain domiciled in Iowa.

18. Plaintiff **Damon Miller** is and at all relevant times was a citizen of the State of Maine and the United States. Miller is a resident of the State of Maine and intends to remain domiciled in Maine.

19. Plaintiff **Carter Bundy** is the next friend and natural parent of his minor son A.B. They are and at all relevant times were citizens of the State of New Mexico and the United States. They are residents of the State of New Mexico and intend to remain domiciled in New Mexico.

20. Plaintiff **Rosa Akhras** is and at all relevant times was a citizen of the State of New Jersey and the United States. Akhras is a resident of the State of New Jersey and intends to remain domiciled in New Jersey.

21. Plaintiff **Srinkanth Alturi** is and at all relevant times was a citizen of the State of New Jersey and the United States. Plaintiff Alturi is a resident of the State of New Jersey and intends to remain domiciled in New Jersey.

22. Plaintiff **Scott Phillips** is the natural parent of his minor son H.P., who is 10 years of age. For purposes of this lawsuit, Phillips has consented to act as a guardian ad litem, and Phillips has no conflict of interest with his minor son. They are and at all relevant times were citizens of the State of New Jersey and the United States. They are residents of the State of New Jersey and intend to remain domiciled in New Jersey.

23. Plaintiff **Corey Benn** is and at all relevant times was a citizen of the State of New York and the United States. Benn is a resident of the State of New York and intends to remain domiciled in New York.

24. Plaintiff **Bellvinia Brickle** is and at all relevant times was a citizen of the Commonwealth of Pennsylvania and the United States. Brickle is a resident of the Commonwealth of Pennsylvania and intends to remain domiciled in Pennsylvania.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists because NextGen and at least one Class Member are citizens of different States. This Court also has supplemental jurisdiction over the claims in this case pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy under Article III of the United States Constitution.

26. The Court has personal jurisdiction over NextGen because NextGen is headquartered in Atlanta, Georgia. NextGen also conducts substantial business in Georgia related to Plaintiffs and Class Members and has thereby established minimum contacts with Georgia sufficient to authorize this Court's exercise of jurisdiction over NextGen.

27. Venue in the Northern District of Georgia is proper under 28 U.S.C. § 1391 because NextGen resides in this District, and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, including NextGen collecting and/or storing the Private Information of Plaintiffs and Class Members.

FACTUAL ALLEGATIONS

NextGen is in the Business of Collecting, Storing, and Maintaining Private Information and Protected Health Information

28. NextGen is a health information technology company and services developer that develops and provides EHR and practice management solutions and services to more than 100,000 healthcare providers who care for more than 65 million patients throughout the United States.[3]

29. NextGen holds itself out as "a leading provider of innovative, cloud-based, healthcare technology solutions that empower healthcare practices to manage the risk and complexity of delivering care in the United States healthcare system."[4]

---

[3] On or about November 7, 2023, NextGen was acquired by Thoma Bravo, a software investment firm, for $1.8 billion. https://www.nextgen.com/company/newsroom/press-release/thoma-bravo-completes-acquisition-of-nextgen-healthcare

[4] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 5, 2023).

30. One of NextGen's most popular EHR and practice management solutions is its NextGen Office software. NextGen Office is a cloud-based platform designed for small to medium-size healthcare providers that combines EHR, practice management, billing, and patient portal functionalities into a single platform.[5]

31. An EHR system, such as NextGen Office, is a system that contains "electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization."[6]

32. EHR systems typically provide the following functions to healthcare providers: (1) identify and maintain a patient records; (2) manage patient demographics; (3) manage problem lists; (4) manage medication lists; (5) manage patient histories; (6) manage clinical documents and notes; (7) capture external clinical documents; (8) present care plans, guidelines, and protocols; (9) manage guidelines, protocols and patient-specific care plans; and (10) generate and record patient-specific instructions.[7] NextGen Office provides many of these EHR system

---

[5] https://www.selecthub.com/medical-software/practice-management/nextgen-office-review/

[6] https://www.hhs.gov/sites/default/files/electronic-health-record-systems.pdf

[7] *Id.*

features.[8]

33. While EHR systems "have transformed healthcare providing convenience and accessibility for patients and providers alike . . . user errors and design flaws make them vulnerable to attack." Put differently, EHR systems, such as NextGen Office, are a one-stop shop for cybercriminals as they contain enticing Private Information and protected health information ("PHI") that is extremely valuable to bad actors with nefarious intentions.[9]

34. As one of the major EHR providers, NextGen advertises that it offers the ability to "[s]ecurely exchange health information" and the ability to focus on patient care "not IT management." NextGen also represents that by using its systems clients are obtaining "world-class security capabilities and system performance."[10]

35. NextGen recognizes the importance of maintaining adequate data security for its NextGen Office system: "If our security measures are breached or fail and unauthorized access is obtained to a client's data, our services may be perceived as not being secure, clients may curtail or stop using our services, and we

---

[8] https://www.nextgen.com/solutions/electronic-health-records/small-practices-nextgen-office

[9] https://thehipaaetool.com/security-risks-of-ehr-and-emr-systems/

[10] https://www.nextgen.com/ (last visited Oct. 16, 2023).

may incur significant liabilities."[11] NextGen highlights its data security to potential customers,[12] promising healthcare providers: "We go to extraordinary lengths to make your data as secure as possible . . . ."[13]

36. Aware of how important data security is to both patients and clients, NextGen in a white paper identifies "Data security threats" as one of the "five tactical and strategic technology challenges that confront medical practices." In its white paper, NextGen informs clients that "the risk in medicine is even greater, as healthcare practices are responsible for the personal health information (PHI) of their patients. PHI is more valuable than credit card or banking data and, therefore, a common target."[14]

37. According to NextGen, "medical practices have good reason to be concerned about the security of their data. In the past three years: 955 major security breaches in healthcare have occurred. 135 million healthcare records have been

---

[11] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 4, 2023).

[12] https://www.nextgen.com/solutions/data-platforms (last visited May 4, 2023).

[13] https://www.nextgen.com/services/managed-cloud (last visited May 4, 2023).

[14] https://nextgen.widen.net/s/hzvtz9nzzk/ne_121019_mcs_datasecurity_whitepaper_lowres (last visited Oct. 16, 2023).

stolen or exposed to unauthorized viewers. 41% of the U.S. population has been affected by healthcare data breaches."[15] NextGen used these real threats, and their consequences, as a marketing point to sell its services.[16]

38. NextGen represented its products as a solution to the problem of data security, touting that it would securely maintain patient data.[17] But that representation proved false.

The Data Breach

39. Between at least March 29, 2023, and April 14, 2023, a hacker infiltrated NextGen's network and accessed and exfiltrated a massive amount of highly sensitive Private Information stored on NextGen systems, including, at least, full names, dates of birth, addresses, and Social Security numbers of patients.

40. While NextGen claims to have discovered the Data Breach on or about March 30, 2023, it did not disclose the existence of the Data Breach until nearly a

---

[15]It is important to note these statistics were from 2018, the problem has only worsened over time.

[16]https://nextgen.widen.net/s/hzvtz9nzzk/ne_121019_mcs_datasecurity_whitepaper_lowres (last visited Oct. 16, 2023).

[17]https://nextgen.widen.net/s/hzvtz9nzzk/ne_121019_mcs_datasecurity_whitepaper_lowres (last visited Oct. 16, 2023).

month later when Defendant began notifying state attorneys general and affected patients on or about April 28, 2023.

41. NextGen has provided minimal information on the Data Breach, claiming only that "an unknown third-party gained unauthorized access to a limited set of electronically stored Private Information" through the use of stolen client credentials and confirming the hacker acquired names, dates of birth, addresses, and/or Social Security numbers of over one million patients.[18]

42. Specifically, NextGen's sample form notification letter provided the following description:

> On March 30, 2023, we were alerted to suspicious activity on our NextGen Office system. In response, we launched an investigation with the help of third-party forensic experts. We also took measures to contain the incident, including resetting passwords, and contacted law enforcement. Based on our in-depth investigation to date, supported by our external experts, it appears that an unknown third-party gained unauthorized access to a limited set of electronically stored Private Information between March 29, 2023 and April 14, 2023. As a result of our detailed analysis of the information impacted, we recently determined that certain of your Private

[18] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023); https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 6, 2023).

> Information was included in the electronic data accessed during the incident. Below we have provided information about what information was involved, what we are doing in response, and what you can do to proactively protect yourself.[19]

43. Based on NextGen's notice sent to patients it is unclear exactly when the sensitive Private Information was taken by the unauthorized third party; when NextGen "launched an investigation" into the Data Breach; the full extent of what data was accessed and/or exposed; when NextGen took action to stop the breach; whether the breach has actually been remediated; and how NextGen confirmed the unauthorized third-parties did not access medical records or medical data contained in NextGen Office while still being able to access valuable Private Information such as Social Security numbers stored *in that same* NextGen Office environment.

44. It is evident that the unauthorized actors accessed the NextGen Office system in an attack designed to acquire sensitive, confidential, and valuable Private Information stored therein, and they were successful in the attack. Based upon NextGen's disclosures, the Private Information stolen by cybercriminals was not encrypted.

---

[19] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last downloaded May 4, 2023).

45. While NextGen has confirmed it detected suspicious activity in its NextGen Office system, NextGen has not provided any information about what other systems within its network were or may have been the subject of unauthorized access. Notably, once hackers find an entry point to a network, they routinely will move laterally (or spread) though the rest of a breached network to other servers, endpoints, and applications.[20]

46. NextGen's notice claims it "took measures to contain the incident, including resetting passwords, and contacted law enforcement."[21] Conspicuously absent from the notice are any specifics on how the breach happened or how NextGen's actions have remediated the root cause.

47. NextGen provides no explanation for why it let the Private Information of Plaintiffs and Class Members sit in the hands of the criminal hackers for nearly a month after NextGen detected the breach before attempting to notify affected patients.

48. By waiting to disclose the Data Breach and by downplaying the risk

---

[20] https://www.cloudflare.com/learning/security/glossary/what-is-lateral-movement/

[21] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).

that victims' Private Information would be misused by criminals, NextGen prevented victims from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

49. NextGen had obligations created by statute, contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

50. Plaintiffs and Class Members entrusted their Private Information to NextGen with the reasonable expectation and mutual understanding that NextGen or anyone who used their Private Information in conjunction with the healthcare services they received would comply with obligations to keep such information confidential and secure from unauthorized access.

51. As a result of the Data Breach, the Private Information of more than 1 million patients—including Plaintiffs and Class Members—was exfiltrated and is now in the hands of criminals.

NextGen Was Breached Not Once, But Twice

52. Despite being a self-described industry leading EHR provider and expressly recognizing the importance of data security, this Data Breach was not the first cybersecurity breach of NextGen's systems this year.

53. On January 17, 2023, NextGen was subjected to a ransomware attack by the ransomware group known as ALPHV/BlackCat.

54. Following the ransomware attack, ALPHV promptly published what is commonly referred to as a "proof pack" on its ransomware leak site.[22] A proof pack is typically used by cybercriminals to put pressure on breached organizations to pay a ransom demand when a ransomware incident or data theft occurs and is intended to show that the hacker possesses the breached data. A proof pack typically reflects a very limited subset of stolen records or portions of the data.

55. The exemplar information leaked in ALPHV's proof pack included nine files consisting of: certain NextGen client contact information, a passport image, NextGen financial data, confidential email communications, and documents related to NextGen's datacenters and data security.

56. Even if a demanded ransom is paid in response to a proof pack, there is no guarantee that stolen data will not be used for nefarious purposes in the future. Security experts warn companies that, even after paying a ransom:

a. the data will not be credibly deleted and that they "should assume it will

[22] https://thecyberexpress.com/nextgen-healthcare-cyber-attack-data-exposed/

be traded to other threat actors, sold, or held for a second/future extortion attempt;"

b. stolen data that was held by multiple parties may not be secured, so even if a threat actor deletes data following a ransom payment, other parties that had access to it may still have copies and use such copies to extort the victim in the future; and

c. the data may be posed before a victim can respond to a ransom demand.[23]

57. Given the difficulty of eliminating malware once it has infiltrated a company's network, the Data Breach may be a continuation of the January 2023 data breach that NextGen failed to discover.

58. In any event, even if the two data breaches are separate and distinct events, the repeated breach of NextGen's systems evinces its flawed data security and its continuous disregard of its obligations to protect Private Information from exposure, compromise, and/or exfiltration by cybercriminals.

59. The January 2023 breach put, or should have put, NextGen on notice

[23] https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/

that further cyberattacks were imminent.

60. Research has indicated that "[r]epeated attacks are actually the norm, not the exception. Some two-thirds (67%) of companies attacked get attacked again within one year." "For ransomware attacks specifically, the number of companies suffering repeated ransomware attacks rose to 80% . . . ."[24]

61. "According to a study by Cybereason, 80% of ransomware victims who paid the ransom were hit by a subsequent ransomware attack, with 68% of compromised organizations saying that the second attack came less than a month later and that the hackers demanded a higher ransom."[25]

62. Repeat cyberattacks are common because during the first attack cybercriminals learn (1) which internal tools are vulnerable to compromise and (2) that such tools can be used to steal customer data. Put differently, once the knowledge of a company's vulnerabilities is made public, cybercriminals are incentivized to engage in a second attack, often targeting the same vulnerabilities as

---

[24] https://securityintelligence.com/articles/how-do-some-companies-get-compromised-again-and-again/

[25] https://techcrunch.com/2023/10/31/ransomware-victims-paying-hackers-ransom/#:~:text=But%20there's%20no%20guarantee%20that,they%20actually%20deleted%20your%20data.

the first attack.[26]

63. Given the success of ALPHV's ransomware attack in January 2023, NextGen was on notice that it would likely be the target of another cyberattack but nevertheless failed to implement adequate data security measures to prevent a second, foreseeable data breach from occurring.

64. Less than 3 months following the announcement of the Data Breach, NextGen was forced to acknowledge another false representation about its NextGen electronic health record system when it agreed to pay $31 million to resolve allegations that NextGen violated the False Claims Act by misrepresenting the capabilities of certain versions of its NextGen medical record software and falsely obtaining certification for its software by hiding that its software lacked critical functionality.[27]

The Data Breach was Foreseeable

65. NextGen was obligated to perform its business operations in

---

[26] https://thecyberexpress.com/nextgen-healthcare-cyber-attack-data-exposed/

[27] https://www.justice.gov/opa/pr/electronic-health-records-vendor-nextgen-healthcare-inc-pay-31-million-settle-false-claims#:~:text=(NextGen)%2C%20an%20electronic%20health,to%20induce%20them%20to%20recommend

accordance with industry standards. Industry standards require NextGen to exercise reasonable care with respect to Plaintiffs and the Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, NextGen was the only entity responsible for adequately protecting the data that they alone solicited, collected, and stored.

66. The injuries to Plaintiffs and Class Members were reasonably foreseeable to NextGen because common law, statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the other Class Members' PII.

67. The injuries to Plaintiffs and the other Class Members also were reasonably foreseeable because NextGen had a cyberattack earlier in the year, NextGen knew or should have known that its systems used for safeguarding PII were inadequately secured and exposed consumer PII to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, NextGen's own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class Members.

68. The injuries to Plaintiffs and the other Class Members also were reasonably foreseeable because NextGen, was aware of the high and ever-increasing incidence of cyberattacks perpetrated against entities that collect PII.

69. As a result, NextGen left Plaintiffs' and Class Members' PII an unguarded target for theft and misuse.

NextGen Had a Duty to Safeguard Class Members' Private Information

70. As part of its business, NextGen undertook to collect, store, and securely maintain Plaintiffs' and Class Members' Private Information, including their PHI.

71. By undertaking to collect, store, and maintain Plaintiffs' and Class Members' Private Information, and deriving monetary benefit from the same, NextGen assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

72. NextGen was fully aware of its obligation to implement and use reasonable measures to protect patients' Private Information.

73. In its 2022 Form 10-K, NextGen states: "Our services involve the storage, transmission and processing of clients' proprietary information and

protected health information of patients. Because of the sensitivity of this information, security features of our software are very important."[28]

74. NextGen's business associate agreements recognize NextGen's duty to "develop, implement, maintain, and use appropriate safeguards to prevent use or disclosure of PHI" and to "reasonably protect PHI from any intentional or unintentional use or disclosure."[29]

75. Indeed, NextGen touts data security as a main feature of its NextGen Office system, stating that it provides "the security and flexibility of web-based tools you can access from your laptop, iPad, or computer"[30] and that NextGen Office is "compliant and has been certified by an ONC-ACB in accordance with the applicable certification criteria adopted by the Secretary of the U.S. Department of Health and Human Services."[31]

76. NextGen's own Privacy Policy provides that NextGen agrees to "use

---

[28] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 5, 2023).

[29] https://www.nextgen.com/-/media/files/legal/2023/d%20-baa%20schedule%20march%202023

[30] https://www.nextgen.com/solutions/electronic-health-records/small-practices-nextgen-office

[31] https://www.nextgen.com/certifications-and-cost-disclosures

reasonably and appropriate security measures designed to protect the personal information we obtain from unauthorized alteration, loss, disclosure, or use, including technological, physical and administrative controls over access to the systems we use to provide . . . our products and services."[32]

77. Additionally, federal agencies have issued recommendations and guidelines for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[33]

78. The FTC's publication "Protecting Private Information: A Guide for Business" sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[34] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of Private Information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e)

---

[32]https://www.nextgen.com/privacy-policy (last visited May 4, 2023).

[33]https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 10, 2023).

[34]https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Oct. 10, 2023).

implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[35]

79. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[36] This is consistent with guidance provided by the Federal Bureau of Investigation ("FBI").

80. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these

---

[35] *Id*.

[36] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 10, 2023.)

actions further clarify the measures businesses must take to meet their data security obligations.[37]

81. Moreover, NextGen is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq.* that provides services to various healthcare providers (i.e., HIPAA "Covered Entities").

82. As a regular and necessary part of its business of providing EHR services, NextGen is responsible for the receipt, custody, and storage of the highly sensitive PHI of its clients' patients.[38]

83. As an entity covered by HIPAA, NextGen is required to implement and maintain sufficient safeguards over its clients' EHRs to protect them from being accessed by unauthorized third parties, including by implementing requirements of the HIPAA Security Rule[39] and to report to the Covered Entities any unauthorized

---

[37] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited May 4, 2023).

[38] Regardless of NextGen's claim that PHI was not involved in this breach, because the PHI was stored in the same system that was breached, *i.e.*, NextGen Office, NextGen's obligations under HIPAA with respect to safeguards required for that system are relevant in assessing NextGen's duty of care in protecting Plaintiffs' and Class Members' Private Information.

[39] The HIPAA Security Rule establishes national standards to protect individuals'

access to, use of, or disclosure of information in patients' EHR.

84. Even though NextGen is required under federal law to maintain the strictest confidentiality of the patients' EHRs, it collected and stored patients' EHRs on the same under-secured and internet-accessible NextGen Office system as the Private Information that was breached here.

85. Several best practices that, at a minimum, should be implemented by healthcare service providers like NextGen, include, but are not limited to: educating all employees on data security; use of strong passwords; enacting multi-layer security, including firewalls, anti-virus, and anti-malware software; ensuring the encryption of data, *i.e.*, making data unreadable without a key; requiring multi-factor authentication; backing-up data; and limiting which individuals can access sensitive data.

86. Other best cybersecurity practices that are standard in the healthcare industry include but are not limited to: installing appropriate malware detection

---

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

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; and training staff regarding critical points.

87. HHS specifically recommends that those in the healthcare industry implement the following cybersecurity practices to protect EHR systems and the patient data contained therein: implementing a zero-trust security model; following the Cybersecurity and Infrastructure Agency measures to protect against potential critical threats (as described below); and generally strengthening an organization's cyber security posture.[40]

88. HHS further recommends the following data security measures a regulated entity such as Nextgen should implement to protect against some of the more common, and often successful, cyber-attack techniques:

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

[40] https://thehipaaetool.com/ehr-cybersecurity-risks/

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

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

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

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

e. Regulated entities should implement strong cyber security practices by

requiring strong passwords rules and multifactor identification.[41]

89. Additionally, 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), are all established standards for reasonable cybersecurity readiness.[42]

90. Plaintiffs and Class Members all are or were patients who received healthcare services from one of NextGen's healthcare provider clients, and who directly or indirectly entrusted NextGen with their Private Information and personal health information stored in its NextGen Office EHR system.

91. By undertaking to obtain, collect, and store Plaintiffs' and Class Members' valuable Private Information, NextGen assumed legal and equitable duties to act reasonably in its collection and storage of the Private Information and

---

[41] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dept't of Health & Human Services (mar. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

[42] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last accessed Oct. 10, 2023)

knew or should have known it was responsible for protecting such Private Information from unauthorized access and exposure.

92. Indeed, NextGen expressly recognizes that it is a custodian of Plaintiffs' and Class Members' Private Information: "In support of the services we provide to your medical professionals, we maintain certain of your personal information on their behalf."[43]

93. NextGen had a duty to act reasonably in collecting, storing, maintaining, and safeguarding Plaintiffs' and Class Members' Private Information and to comply with the existing and applicable cybersecurity standards in the healthcare industry.

94. To prevent and detect unauthorized cyber-attacks, such as the Data Breach, the Federal Bureau of Investigation recommends the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the

[43] https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 6, 2023).

end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop Protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational

units.[44]

95. Further, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, the United States Cybersecurity & Infrastructure Security Agency recommends the following measures:

a. **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

b. **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in

[44] *Id.* at 3-4.

spelling or a different domain (e.g., .com instead of .net).

c. **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d. **Keep your Private Information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it….

e. **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f. **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

g. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to

reduce malicious network traffic….[45]

96. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach the Microsoft Threat Protection Intelligence Team recommends the following measures:

Secure internet-facing assets

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;

---

[45]See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed Oct. 10, 2023).

- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[46]

NextGen's Actions and Inactions Caused the Data Breach

97. Data disclosures and data breaches are preventable.[47] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[48] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised [.]"[49]

---

[46]See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at https://www.microsoft.com/security/blog/2020/03/05/human-operatedransomware-attacks-a-preventable-disaster/ (last accessed Oct. 10, 2023).

[47]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[48]*Id.* at 17.

[49]*Id.* at 28.

98. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[50]

99. NextGen could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Additionally, NextGen could have destroyed the data, at least for individuals with whom it had not had a relationship for a period of time.

100. NextGen's negligence in affirmatively mishandling its data security, instituting inaccurate security controls, and improperly maintaining and safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like NextGen to protect and secure sensitive data they possess.

101. Despite the prevalence of public announcements of data breach and data security compromises, NextGen took insufficient steps to protect the Private

---

[50] *Id.* (emphasis added).

Information of Plaintiffs and Class Members from being compromised.

102. NextGen instituted inadequate security controls and products and/or failed to institute the controls and products that would prevent the Data Breach, including those security controls and products recommended by the FBI.

103. NextGen instituted inadequate security controls and products and/or failed to institute the controls and products that would prevent the Data Breach, including those security controls and products recommended by the United States Cybersecurity & Infrastructure Security Agency.

104. NextGen instituted inadequate security controls and products and/or failed to institute the controls and products that would prevent the Data Breach, including those security controls and products recommended by the Microsoft Threat Protection Intelligence Team.

105. Given that NextGen was storing the Private Information and PHI of at a minimum, one million individuals, NextGen could have and should have implemented sufficient data security controls and measures, including all of the measures described above, to prevent and detect cyberattacks.

106. Upon information and belief, however, NextGen improperly implemented and/or failed to implement the above-described data security measures and affirmatively mishandled the maintenance of the Private Information with which

it was entrusted, leading to the Data Breach.

107. NextGen affirmatively breached its obligations and duties to Plaintiffs and Class Members and/or was otherwise negligent because it mismanaged its data security systems and policies, failing to adequately safeguard Plaintiffs' and Class Members' Sensitive Information.

108. Upon information and belief, NextGen's unlawful conduct included, but is not limited to, one or more of the following affirmative acts and/or omissions:

a. Acting unreasonably in collecting, storing, and maintaining the Private Information and failing to exercise reasonable care in its implementation of its security systems, protocols, and practices in order to sufficiently protect the Private Information of Plaintiffs and Class Members;

b. Negligently designing and maintaining its data security system in a manner that failed secure Plaintiffs' and Class Members' Private Information from unauthorized access;

c. Implementing inadequate security controls;

d. Implementing inadequate security products;

e. Implementing inadequate security policies, including with respect to password protection policies and use of multi-factor authentication for its clients that use its systems;

f. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

g. Failing to test and assess the adequacy of its data security system;

h. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

i. Failing to develop and put into place uniform procedures and data security protections for its healthcare network;

j. Allocating insufficient funds and resources to the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

k. Failing to ensure that it was compliant with FTC guidelines for cybersecurity;

l. Failing to ensure that it was adhering to one or more of industry standards for cybersecurity discussed above;

m. Failing to implement or update antivirus and malware protection software in need of security updating;

n. Designing its systems without encryption or without adequate encryption of the Private Information;

o. Designing its systems in a manner that did not require clients to use

multi-factor authentication or require forced password changes;

p. Failing to comply with its own Privacy Policy;

q. Failing to comply with regulations protecting the Private Information at issue during the period of the Data Breach;

r. Failing to recognize in a timely manner that Private Information had been compromised;

s. Waiting for a month before it disclosed the Data Breach; and

t. Otherwise mishandling Plaintiffs' and Class Members' Private Information provided to NextGen, which in turn allowed cyberthieves to access its NextGen Office system.

109. This Data Breach would not have occurred, and Plaintiffs' and Class Members' Private Information would not be in the hands of criminals, but for NextGen's mishandling of its data security.

NextGen Knew the Risks of Storing Plaintiffs' and Class Members' Private Information and the Harm to Plaintiffs and Class Members as a Result of the Data Breach was Foreseeable and Preventable

110. In response to the Data Breach, NextGen stated it "launched an

investigation with the help of third-party forensic experts."[51]

111. But NextGen, like any company of its size that stores massive amounts of sensitive personal data, should have had robust protections in place to detect and terminate a successful intrusion long before a hacker could access and exfiltrate over one million patient files.

112. NextGen's only disclosed tangible response to the Data Breach was to "reset[] passwords." If the Data Breach was so easily contained or remediated, NextGen's failure to prevent the Data Breach is inexcusable given its knowledge that it was a prime target for cyberattacks.

113. Its status as a prime target for cyberattacks was known and obvious to NextGen as disclosed in its own regulatory filings.[52]

114. NextGen fully understood that the type of information it collects, maintains, and stores is highly coveted and a frequent target of hackers.[53]

115. In its 2022 form 10-K NextGen acknowledged this danger:

---

[51] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).

[52] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last downloaded May 4, 2023).

[53] https://nextgen.widen.net/s/hzvtz9nzzk/ne_121019_mcs_datasecurity_whitepaper_lowres (Last accessed Oct. 17, 2023).

> High-profile security breaches at other companies have increased in recent years, and security industry experts and government officials have warned about the risks of hackers and cyber-attacks targeting information technology products and businesses. Although this is an industry-wide problem that affects other software and hardware companies, we may be targeted by computer hackers because we are a prominent healthcare information technology company and have high profile clients. These risks will increase as we continue to … store and process increasingly large amounts of our client's confidential data, including personal health information…. Moreover, unauthorized access, use or disclosure of such sensitive information, including any resulting from the incidents described above, could result in civil or criminal liability or regulatory action, including potential fines and penalties. … These types of security incidents could also lead to lawsuits, regulatory investigations and claims, and increased legal liability.[54]

116. In August 2018, NextGen's current Chief Information and Security Officer, David Slazyk, published a blog post on NextGen's website titled "Two essential ways to make your practice data more secure."[55]

117. Mr. Slazyk represented that "At NextGen Healthcare we are committed

---

[54]https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 5, 2023).

[55]https://www.nextgen.com/blog/make-your-practice-data-more-secure (last visited May 5, 2023).

to … Using the most advanced security controls available…"[56] He also represented that healthcare providers "can off-load the task of data protection to NextGen Healthcare by taking advantage of [NextGen's] services."[57]

118. NextGen knew or should have known that its data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry preceding the Data Breach.

119. The healthcare industry specifically is a prime target for threat actors. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights."[58]

120. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent

---

[56] *Id*.

[57] *Id*.

[58] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/, (last visited Oct. 16, 2023).

of all reported incidents.[59]

121. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and, as of 2022, healthcare data breach costs have hit a new record high.[60]

122. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[61]

123. While EHR systems such as NextGen's have helped to revolutionize recordkeeping of patient information, they are also an Achillies heel for maintaining privacy. The Department of Health and Human Services ("HHS") has reported that some of the largest healthcare data breaches in 2022 were linked to third party vendors, including EHR providers, such as Eye Care Leaders (EHR and practice management systems, 3.6 million individuals) and Connexin Software, Inc. (EHR

---

[59] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited October 5, 2022).

[60] *Cost of a Data Breach Report 2022*, IBM Security, available: https://www.ibm.com/downloads/cas/3R8N1DZJ.

[61] See Maria Hernandez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

and practice management software provider, 2.2 million individuals).

124. Recognizing the risks EHR systems pose to patient information, HHS has now twice published threat briefs about the cybersecurity risks of EHR systems. HHS warns that EHR systems, like NextGen Office, are top targets for cybercriminals because not only are they vulnerable to attack, but they also contain extremely valuable information that cybercriminals can profit from on the dark web or black market.[62]

125. Because of the value of the type of data the medical industry collects and stores, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, NextGen knew or should have known the serious risk of a data breach and the resulting harm and strengthened its data security accordingly.

126. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including,

---

[62] https://thehipaaetool.com/ehr-cybersecurity-risks/

among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[63]

127. Data breaches and the harm they cause have become so common and notorious the FTC has issued warnings about the destruction caused by an unauthorized person having access to someone's Private Information, stating: "Once identity thieves have your Private Information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[64]

128. At all relevant times, NextGen knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences and harm that would occur to patients if its data security system was breached and their Private Information exposed to criminals, including the

---

[63] *See generally* Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business, FED. TRADE COMM., https://www.ftc.gov/businessguidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed Oct. 10, 2023).

[64] https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last accessed May 4, 2023).

significant costs that would be imposed on individual patients as a result of a breach.

129. NextGen was, or should have been, fully aware of the significant number of patients whose Private Information it collected, and thus, the significant number of patients who would be harmed by a breach of its systems.

130. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including OneTouchPoint, Inc. (4.1 million patients, July 2022), Shields Healthcare Group (2 million patients, March 2022), Blackbaud, Inc. (millions of individuals, May 2020), American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

131. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets to be aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have

lesser IT defenses and a high incentive to regain access to their data quickly." [65]

132. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[66]

133. NextGen was on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[67]

134. The American Medical Association ("AMA") has also warned

---

[65]FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targetedransomware

[66]https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Oct. 10, 2023).

[67] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[68]

135. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

136. Moreover, NextGen was keenly aware of its status as a prime target because it had in fact been victimized earlier this year, making NextGen more susceptible to another imminent attack.[69]

137. While NextGen issued a statement in response to the January 2023 attack claiming "[t]he privacy and security of our client information is of the utmost

---

[68] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

[69] https://www.washingtonpost.com/politics/2023/01/23/latest-cyberattack-health-care-shows-how-vulnerable-sector-is/ (last visited May 5, 2023).

importance to us," NextGen continued to mishandle its data security and failed to identify the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patients' Private Information that resulted in the Data Breach and the compromise of that Private Information.[70]

138. Had NextGen implemented common sense security measures, the Data Breach, and the resulting foreseeable harm to over one million patients whose Private Information was compromised, would have been prevented.

The Value of Private Information

139. The Private Information of consumers has a high value to criminals, as evidenced by the prices offered for such information on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, according to the 2021 Dark Web Price Index, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[71] The same report shows payment card details for an account balance up to $1,000 have an

---

[70] *Id.*

[71] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[72] Similarly, according to the Infosec Institute Private Information can sell for as much as $363 per record.[73]

140. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts, a fact NextGen itself recognizes.[74]

141. The Private Information exposed in the Data Breach is valuable to identity thieves for use in the kinds of criminal activity described below. These risks are both certainly impending and substantial. As the FTC has reported, if cyber

---

[72]Dark Web Price Index 2021, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/

[73]See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Oct. 10, 2023).

[74]https://nextgen.widen.net/s/hzvtz9nzzk/ne_121019_mcs_datasecurity_whitepaper_lowres (last accessed Oct. 17, 2023).

thieves get access to a person's highly sensitive information, they will use it.[75]

142. Social Security numbers are among the worst kinds of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the victim, requiring a wholesale review of the victim's relationships with government agencies and any number of private companies in order to update the victim's accounts with those entities.

143. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other Private Information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your

---

[75] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

> Social Security number and assuming your identity can cause a lot of problems.[76]

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

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other Private Information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[77]

145. Social Security numbers allow individuals to apply for credit cards,

---

[76] https://www.ssa.gov/pubs/EN-05-10064.pdf

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

student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of Private Information to steal and then sell.

146. This was a financially motivated Data Breach; the reason cybercriminals such as the bad actors here go through the trouble of running a targeted cyberattack against companies like NextGen is to obtain information that they can monetize such as by selling it on the black market for use in the kinds of criminal activity described herein.

147. The Private Information at issue here demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black

market."[78]

148. According to another source, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[79] And, "if there is reason to believe that your Private Information has been stolen, you should assume that it can end up for sale on the dark web."[80]

149. Private Information is a valuable property right.[81] Its value is axiomatic, considering the value of Big Data in corporate America and the fact that convictions for cyber theft can include heavy prison sentences.

---

[78]Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-datastolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Oct. 10, 2023)

[79] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017,

https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[80] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[81]See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15Rich. 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).

150. There is also an active and robust legitimate market for some of the personal information at issue in this case. Marketing firms utilize Private Information to target potential customers, and data brokers constantly set trading markets that value personal data.

151. In 2019, the data brokering industry was worth roughly $200 billion.[82] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[83] For example, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[84]

152. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used.

153. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[82]https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[83]https://datacoup.com/

[84]Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[85]

154. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[86]

Plaintiffs' Experiences With the Data Breach

California
Plaintiff Alvarado

155. Plaintiff Alvarado is and at all relevant times was a citizen of the State of California and the United States.

156. Plaintiff Alvarado was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Alvarado was required to provide and entrust NextGen with her Private Information. When providing and

---

[85]Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last accessed Oct. 10, 2023).

[86] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

entrusting NextGen with her Private Information, Plaintiff Alvarado reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

157. In or about April or May, 2023, Plaintiff Alvarado received a notification letter from NextGen stating that she was a victim of the Data Breach. The letter recommended that Plaintiff Alvarado take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Alvarado and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

158. To protect against additional harm, Plaintiff Alvarado has and will take precautions to mitigate the risk of future identity theft and fraud. These precautions include spending time and effort reviewing her credit profile and financial and other account statements for evidence of unauthorized activity, much of which Plaintiff Alvarado will need to continue indefinitely to protect herself from harm resulting from the Data Breach.

159. Despite taking the precautionary measures and staying vigilant as

recommended in the Data Breach notification letter, Plaintiff Alvarado has already experienced the effects of the dissemination of her Private Information on the Dark Web. As a result of the Data Breach, a bad actor has attempted to gain access to Plaintiff Alvarado's bank account, forcing her to close the account. In addition, Plaintiff Alvarado's credit score dropped as a result of bad actors doing hard pulls of her credit report. Plaintiff Alvarado has also seen an increase in spam texts and phone calls since the breach.

160. To date, Plaintiff Alvarado has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Alvarado values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

161. Had Plaintiff Alvarado been informed of NextGen's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Alvarado has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Alvarado anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

162. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Alvarado faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

163. Upon information and belief, NextGen continues to store and/or share Plaintiff Alvarado's Private Information on its internal systems. Thus, Plaintiff Alvarado has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Plaintiff Appleton

164. Plaintiff Appleton is and at all relevant times was a citizen of the State of California and the United States.

165. Plaintiff Appleton was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Appleton was required to provide and entrust NextGen with her Private Information. When providing and entrusting NextGen with her Private Information, Plaintiff Appleton reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

166. In or about April or May, 2023, Plaintiff Appleton received a

notification letter from NextGen stating that she was a victim of the Data Breach.

167. The letter recommended that Plaintiff Appleton take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Appleton and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

168. Since learning about the Data Breach, Plaintiff Appleton has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include spending time and effort reviewing her credit profile and financial and other account statements for evidence of unauthorized activity, much of which Plaintiff Appleton will need to continue indefinitely to protect herself from harm resulting from the Data Breach.

169. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Appleton has already experienced the effects of the dissemination of her Private Information on the Dark Web. As a result of the breach, some bad actor(s) began harassing Plaintiff Appleton, by repeatedly spamming her with phone calls and sending unwanted food deliveries

to her house. This harassment was near constant for two to three weeks. In addition to the harassment, after she enrolled in the "free" Experian credit monitoring offered by NextGen, Plaintiff Appleton was charged $24.99 for the service.

170. To date, Plaintiff Appleton has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Appleton values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

171. Had Plaintiff Appleton been informed of NextGen's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Appleton has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Appleton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

172. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Appleton faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the

indefinite future.

173. Upon information and belief, NextGen continues to store and/or share Plaintiff Appleton's Private Information on its internal systems. Thus, Plaintiff Appleton has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Georgia
Plaintiff Abikoye

174. Plaintiff Abikoye is and at all relevant times was a citizen of the State of Georgia and the United States.

175. Plaintiff Abikoye was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Abikoye was required to provide and entrust NextGen with her Private Information. When providing and entrusting NextGen with her Private Information, Plaintiff Abikoye reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

176. In or about April or May 2023, Plaintiff Abikoye received a notification letter from NextGen stating that she was a victim of the Data Breach.

177. The letter recommended that Plaintiff Abikoye take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements

and credit reports closely." Despite making these recommendations to Plaintiff Abikoye and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

178. Since learning about the Data Breach, Plaintiff Abikoye has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include purchasing credit monitoring, placing freezes on her credit, placing a pin with the IRS on her tax return, and checking her accounts for fraudulent activity, much of which Plaintiff Abikoye will need to continue indefinitely to protect herself from harm resulting from the Data Breach.

179. Plaintiff Abikoye has spent multiple hours and at least $120 on Aura credit monitoring services and otherwise expended efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Abikoye values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

180. Had Plaintiff Abikoye been informed of NextGen's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to NextGen. Given the highly sensitive nature of

the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Abikoye has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Abikoye anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

181. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Abikoye faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

182. Upon information and belief, NextGen continues to store and/or share Plaintiff Abikoye's Private Information on its internal systems. Thus, Plaintiff Abikoye has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Illinois
Plaintiff Bailey

183. Plaintiff Bailey is and at all relevant times was a citizen of the State of Illinois and the United States.

184. Plaintiff Bailey was a patient at one or more of NextGen's healthcare

clients. In order to receive healthcare services, Plaintiff Bailey was required to provide and entrust NextGen with her Private Information. When providing and entrusting NextGen with her Private Information, Plaintiff Bailey reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

185. In or about April or May, 2023, Plaintiff Bailey received a notification letter from NextGen stating that she was a victim of the Data Breach.

186. The letter recommended that Plaintiff Bailey take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Bailey and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

187. Since learning about the Data Breach, Plaintiff Bailey has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include spending time and effort reviewing her credit profile and financial and other account statements for evidence of unauthorized activity, much of which Plaintiff Bailey will need to continue indefinitely to protect herself from harm resulting from

the Data Breach.

188. To date, Plaintiff Bailey has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Bailey values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

189. Had Plaintiff Bailey been informed of NextGen's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Bailey has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Bailey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

190. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Bailey faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

191. Upon information and belief, NextGen continues to store and/or share

Plaintiff Bailey's Private Information on its internal systems. Thus, Plaintiff Bailey has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Iowa
Plaintiff Kerr

192. Plaintiff Kerr is the natural parent of her minor child J.K. who is and at all relevant times was a citizen of the State of Iowa and the United States.

193. Plaintiff Kerr's child was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Kerr was required to provide and entrust NextGen with her child's Private Information. When providing and entrusting NextGen with her child's Private Information, Plaintiff Kerr reasonably expected that her child's Private Information would remain safe and not be accessed by unauthorized third parties.

194. Plaintiff Kerr received a notification letter on or about May or June 2023 from NextGen stating that her son was a victim of the Data Breach.

195. The letter recommended that Plaintiff Kerr take certain actions like monitoring accounts and "remain vigilant by reviewing your child's account statements and credit reports closely." Despite making these recommendations to Plaintiff Kerr and the other victims of the Data Breach, NextGen itself was not

vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

196. Since learning about the Data Breach, Plaintiff Kerr has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include researching the Data Breach.

197. To date, Plaintiff Kerr has spent approximately five hours on efforts to react to and protect her child from harm resulting from the Data Breach. Plaintiff Kerr values her child's privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

198. Had Plaintiff Kerr been informed of NextGen's insufficient data security measures to protect her child's Private Information, she would not have willingly provided her child's Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Kerr anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

199. Given the nature of the information exposed in the Data Breach and the

propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Kerr's child faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

200. Upon information and belief, NextGen continues to store and/or share Plaintiff Kerr's child's Private Information on its internal systems. Thus, Plaintiff Kerr has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Maine
Plaintiff Miller

201. Plaintiff Miller is and at all relevant times was a citizen of the State of Maine and the United States.

202. Plaintiff Miller was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Miller was required to provide and entrust NextGen with his Private Information. When providing and entrusting NextGen with his Private Information, Plaintiff Miller reasonably expected that his Private Information would remain safe and not be accessed by unauthorized third parties.

203. Plaintiff Miller received a notification letter from NextGen dated April

28, 2023, stating that he was a victim of the Data Breach.

204. The letter recommended that Plaintiff Miller take certain actions like monitoring his accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Miller and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

205. Since learning about the Data Breach, Plaintiff Miller has taken precautions to mitigate the risk of future identity theft and fraud. These precautions included researching the details of the Data Breach, enrolling in the credit monitoring program offered in the notice letter, reviewing financial accounts, and blocking spam calls and texts, much of which Plaintiff Miller will need to continue indefinitely to protect himself from harm resulting from the Data Breach.

206. Despite taking these precautionary measures and staying vigilant, as recommended in the Data Breach notification letter, Plaintiff Miller has already experienced the effects of the dissemination of his Private Information on the Dark Web. Plaintiff Miller has experienced an increase in scam phishing calls and text messages.

207. To date, Plaintiff Miller has spent time on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Miller values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

208. Had Plaintiff Miller been informed of NextGen's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Miller has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Miller anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

209. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Miller faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

210. Upon information and belief, NextGen continues to store and/or share Plaintiff Miller's Private Information on its internal systems. Thus, Plaintiff Miller

has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

New Jersey
Plaintiff Alturi

211. Plaintiff Alturi is and at all relevant times was a citizen of the State of New Jersey and the United States.

212. Plaintiff Alturi was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Alturi was required to provide and entrust NextGen with his Private Information. When providing and entrusting NextGen with his Private Information, Plaintiff Alturi reasonably expected that his Private Information would remain safe and not be accessed by unauthorized third parties.

213. Plaintiff Alturi received a notification letter from NextGen dated April 28, 2023, stating that he was a victim of the Data Breach.

214. The letter recommended that Plaintiff Alturi take certain actions like monitoring his accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Alturi and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage

of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

215. Since learning about the Data Breach, Plaintiff Alturi has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include researching the data breach, reviewing his financial accounts, freezing his credit with all three bureaus, and reporting and responding to two incidents of fraud, as discussed below. Plaintiff Alturi will need to continue indefinitely to take steps to protect himself from harm resulting from the Data Breach.

216. Despite taking these precautionary measures and staying vigilant, as recommended in the Data Breach notification letter, Plaintiff Alturi has already experienced the effects of the theft of his Private Information and dissemination of his Private Information on the Dark Web. Notably, following the Data Breach, on two separate occasions, an unauthorized third party opened a savings account in his name at Bank of America. In response, Plaintiff Alturi was forced to spend time filing fraud reports with the bank and reporting the fraud to the FTC.

217. To date, Plaintiff Alturi has spent over three hours of time on mitigation efforts to react to and protect himself from the harm resulting from the Data Breach. Plaintiff Alturi values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

218. Had Plaintiff Alturi been informed of NextGen's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Alturi has already suffered injury and remains at a current, substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Alturi anticipates spending considerable time on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

219. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Alturi faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

220. Upon information and belief, NextGen continues to store and/or share Plaintiff Alturi's Private Information on its internal systems. Thus, Plaintiff Alturi has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Plaintiff Akhras

221. Plaintiff Akhras is and at all relevant times was a citizen of the State of

New Jersey and the United States.

222. Plaintiff Akhras was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Akhras was required to provide and entrust NextGen with her Private Information. When providing and entrusting NextGen with her Private Information, Plaintiff Akhras reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

223. In or about April or May 2023, Plaintiff Akhras received a notification letter from NextGen stating that she was a victim of the Data Breach.

224. The letter recommended that Plaintiff Akhras take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Akhras and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

225. Since learning about the Data Breach, Plaintiff Akhras has taken precautions to mitigate the risk of future identity theft and fraud. These precautions included researching the data breach, reviewing her financial accounts, freezing her

credit, working with her bank to change her account passwords and account information, and purchasing credit monitoring services. Plaintiff Akhras will need to continue indefinitely to take steps to protect herself from harm resulting from the Data Breach.

226. Despite taking these precautionary measures and staying vigilant, as recommended in the Data Breach notification letter, Plaintiff Akhras has already experienced the effects of the theft of his Private Information and dissemination of her Private Information on the Dark Web. Notably, following the Data Breach, Plaintiff Akhras was contacted by her bank regarding a fraudulent withdrawal from her checking account. In response, Plaintiff Akhras worked with her bank to change her passwords and account information. Despite this effort, bad actors again accessed her bank accounts and stole additional money. Additionally, bad actors in an attempt to open fraudulent credit cards initiated hard inquiries on Plaintiff Akhras's credit that have lowered her credit score. In response to this and the Data Breach, Plaintiff Akhras spent time and effort to freeze her credit.

227. To date, Plaintiff Akhras has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Akhras values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

228. Had Plaintiff Akhras been informed of NextGen's insufficient data security measures to protect her Private Information, she would not have willingly provided his Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Akhras has already suffered injury and remains at a current, substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Akhras anticipates spending considerable time on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

229. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Akhras faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

230. Upon information and belief, NextGen continues to store and/or share Plaintiff Akhras's Private Information on its internal systems. Thus, Plaintiff Akhras has a continuing interest in ensuring that the Private information is protected and safeguarded from future breaches.

Plaintiff Phillips

231. Plaintiff Phillips is the natural parent of his minor child H.P. who is and

at all relevant times was a citizen of the State of New Jersey and the United States.

232. Plaintiff Phillips's child was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Phillips was required to provide and entrust NextGen with his child's Private Information. When providing and entrusting NextGen with his child's Private Information, Plaintiff Phillips reasonably expected that his child's Private Information would remain safe and not be accessed by unauthorized third parties.

233. Plaintiff Phillips received a notification letter from NextGen on or about April 28, 2023, stating that his son was a victim of the Data Breach.

234. The letter recommended that Plaintiff Phillips take certain actions like monitoring accounts and "remain vigilant by reviewing your child's account statements and credit reports closely." Despite making these recommendations to Plaintiff Phillips and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

235. Since learning about the Data Breach, Plaintiff Phillips has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include spending time and effort reviewing his son's credit profile and other financial

information and accounts for evidence of unauthorized activity, which he will continue to do indefinitely.

236. To date, Plaintiff Phillips has spent multiple hours on efforts to react to and protect his child from harm resulting from the Data Breach. Plaintiff Phillips values his child's privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

237. Had Plaintiff Phillips been informed of NextGen's insufficient data security measures to protect his child's Private Information, he would not have willingly provided his child's Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Phillips anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

238. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Phillips's child faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

239. Upon information and belief, NextGen continues to store and/or share Plaintiff Phillips's child's Private Information on its internal systems. Thus, Plaintiff Phillips has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

New Mexico
Plaintiff Bundy

240. Plaintiff Bundy is the natural parent of his minor child A.B., who is and at all relevant times was a citizen of the State of New Mexico and the United States.

241. Plaintiff Bundy's child was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Bundy was required to provide and entrust NextGen with his child's Private Information. When providing and entrusting NextGen with his child's Private Information, Plaintiff Bundy reasonably expected that his child's Private Information would remain safe and not be accessed by unauthorized third parties.

242. Plaintiff Bundy received a notification letter dated April 28, 2023, from NextGen stating that his minor child was a victim of the Data Breach.

243. The letter recommended that Plaintiff Bundy take certain actions like monitoring accounts and "remain vigilant by reviewing your child's account statements and credit reports closely." Despite making these recommendations to

Plaintiff Bundy and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

244. Since learning about the Data Breach, Plaintiff Bundy has taken precautions to mitigate the risk of future identity theft and fraud. These precautions include researching the Data Breach and reviewing accounts, much of which Plaintiff Bundy will need to continue indefinitely to protect his child from harm resulting from the Data Breach.

245. To date, Plaintiff Bundy has spent approximately one hour on efforts to react to and protect his child from harm resulting from the Data Breach. Plaintiff Bundy values his son's privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

246. Had Plaintiff Bundy been informed of NextGen's insufficient data security measures to protect his child's Private Information, he would not have willingly provided his child's Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff

Bundy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Bundy's child faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

247. Upon information and belief, NextGen continues to store and/or share Plaintiff Bundy's child's Private Information on its internal systems. Thus, Plaintiff Bundy has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

New York
Plaintiff Benn

248. Plaintiff Benn is and at all relevant times was a citizen of the State of New York and the United States.

249. Plaintiff Benn was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Benn was required to provide and entrust NextGen with his Private Information. When providing and entrusting NextGen with his Private Information, Plaintiff Ben reasonably expected that his Private Information would remain safe and not be accessed by unauthorized third

parties.

250. Plaintiff Ben received a notification letter from NextGen dated April 28, 2023, stating that he was a victim of the Data Breach.

251. The letter recommended that Plaintiff Benn take certain actions like monitoring his accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Benn and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

252. Since learning about the Data Breach, Plaintiff Benn has taken precautions to mitigate the risk of future identity theft and fraud. These precautions included researching the Data Breach, reviewing financial accounts, and paying money for additional fraud protection, much of which Plaintiff Ben will need to continue indefinitely to protect himself from harm resulting from the Data Breach.

253. To date, Plaintiff Ben has spent approximately 10 hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Benn values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

254. Had Plaintiff Benn been informed of NextGen's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Benn has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Benn anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

255. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Benn faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

256. Upon information and belief, NextGen continues to store and/or share Plaintiff Benn's Private Information on its internal systems. Thus, Plaintiff Benn has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

Pennsylvania
Plaintiff Brickle

257. Plaintiff Brickle is and at all relevant times was a citizen of the Commonwealth of Pennsylvania and the United States.

258. Plaintiff Brickle was a patient at one or more of NextGen's healthcare clients. In order to receive healthcare services, Plaintiff Brickle was required to provide and entrust NextGen with her Private Information. When providing and entrusting NextGen with her Private Information, Plaintiff Brickle reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

259. On or about May 4, 2023, Plaintiff Brickle received a notification letter from NextGen stating that she was a victim of the Data Breach.

260. The letter recommended that Plaintiff Brickle take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements and credit reports closely." Despite making these recommendations to Plaintiff Brickle and the other victims of the Data Breach, NextGen itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. NextGen's lack of vigilance and care directly led to the Data Breach.

261. Since learning about the Data Breach, Plaintiff Brickle has taken precautions to mitigate the risk of future identity theft and fraud. These precautions

include spending time and effort reviewing her credit profile and financial and other account statements for evidence of unauthorized activity, which she will continue to do indefinitely.

262. To date, Plaintiff Brickle has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Brickle values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

263. Had Plaintiff Brickle been informed of NextGen's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to NextGen. Given the highly sensitive nature of the Private Information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Brickle has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Brickle anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

264. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Brickle faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite

future.

265. Upon information and belief, NextGen continues to store and/or share Plaintiff Brickle's Private Information on its internal systems. Thus, Plaintiff Brickle has a continuing interest in ensuring that the Private Information is protected and safeguarded from future breaches.

The Impact of the Data Breach on Plaintiffs and Class Members

266. NextGen's negligent handling of Plaintiffs' and Class Members' Private Information has severe and long-lasting ramifications. Given the sensitive nature of the Private Information stolen in the Data Breach—names, date of birth, addresses and Social Security numbers—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

267. As discussed above, the Private Information exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. With access to an individual's Private Information, malicious actors can use Private Information to, among other things, gain access to consumers' bank accounts, social media, and credit cards.

268. Malicious actors can also use consumers' Private Information to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[87]

269. Further, malicious actors often wait months or years to use the Private Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Private Information, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

270. For example, it is believed that certain highly sensitive Private Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[88]

---

[87]A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

[88] Brian Krebs, *U.S. Secret Service: "Massive Fraud" against State Unemployment Insurance Programs*, KrebsonSecurity (May 16, 2020), https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/; Lilly Hay Newman, *The Nigerian*

271. Victims of the Data Breach face significant harms as the result of the Data Breach, including, but not limited to, actual identity theft and fraud as well as substantial and imminent risk of identity theft and fraud. Plaintiffs and Class Members are forced to spend time, money, and effort reacting to and dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for and responding to unauthorized activity.

272. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% report problems with family members as a result of the

Fraudsters Ripping Off the Unemployment System, Wired (May 19, 2020), https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

breach; and

- 10% reported feeling suicidal.[89]

273. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[90]

274. The unauthorized disclosure of sensitive Private Information to data

---

[89] https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited May 4, 2023).

[90] https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited May 4, 2023).

thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[91]

275. Plaintiffs are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that are aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's Private Information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

276. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to the following:

a. the unconsented disclosure of confidential information to a third party;

---

[91] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

b. losing the inherent value of their Private Information;

c. losing the value of access to their Private Information permitted without authorization by NextGen;

d. identity theft and fraud resulting from the theft of their Private Information;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

g. the present value of ongoing credit monitoring and identity theft protection services necessitated by NextGen's Data Breach;

h. unauthorized charges and loss of use of and access to their accounts;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the

Data Breach; and

k. the continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being in the possession of one or many unauthorized third parties.

277. As a result of the actual and imminent risk of identity theft Plaintiffs and Class Members must, as NextGen's Notice instructs them, "remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements, explanation of benefits, and free credit reports for unexpected activity or errors over the next 12 to 24 months." In fact, such vigilance against identity theft and fraud will be required for the remainder of Plaintiffs' and Class Members' lifetimes.

278. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent mitigative actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports.

279. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs

and time to repair the damage to their good name and credit record."[92]

280. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[93]

281. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that victim whole again as there is typically significant time and effort associated with seeking reimbursement.

282. Plaintiffs and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important

---

[92]See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[93]See Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited Oct. 10, 2023).

consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less Private Information to organizations that suffered a data breach.[94]

283. Likewise, the American Bankers Association, reporting on a global consumer survey regarding concerns about privacy and data security, noted that 29% of consumers would avoid using a company that had experienced a data breach, with 63% of consumers indicating they would avoid such a company for a period of time.[95]

284. Plaintiffs and Class Members have a direct interest in NextGen's promises and duties to protect their Private Information, *i.e.*, that NextGen not increase their risk of identity theft and fraud.

285. Because NextGen failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and

---

[94]https://web.archive.org/web/20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited May 4, 2023).

[95]https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/ (last visited May 4, 2023).

continuing increased risk of harm caused by NextGen's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class Members as close to the same position as they would have occupied but for NextGen's wrongful conduct, namely its failure to adequately protect Plaintiffs' and Class Members' Private Information.

286. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their Private Information permitted through NextGen's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's Private Information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology.

287. Nevertheless, Plaintiffs may generally recover the reasonable use value of the improperly used information—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such information to the infringer.

288. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value.

This measure is appropriate because (a) Plaintiffs and Class Members have a protectible interest in their Private Information; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

289. NextGen's delayed notice letter also caused Plaintiffs and Class Members harm. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. NextGen's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk.

290. By waiting nearly a month to disclose the Data Breach and by downplaying the risk of misuse, NextGen prevented victims from taking meaningful, proactive, and targeted mitigation measures to secure their Private Information and accounts.

291. These injuries to Plaintiffs and Class Members were directly and proximately caused by NextGen's failure to implement or maintain adequate data security measures for the victims of the Data Breach.

292. Further, because NextGen continues to hold their Private Information,

Plaintiffs and Class Members have an interest in ensuring that their Private Information is secured and not subject to further theft.

The Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

293. To date, NextGen has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. NextGen has only offered twenty-four (24) months of inadequate identity monitoring services through Experian's Identity Works, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the foreseeable future. NextGen has not offered any other relief or protection. The 24 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

294. Victims of data breaches often elect not to enroll in a monitoring product offered by the very entity that compromised their data. In other words, an offer of monitoring of the type made by NextGen in the wake of a breach is typically viewed with skepticism by the victims of breach because it requires victims to provide additional information to the vendor of the breached party.

295. In any event, NextGen puts the onus on Plaintiffs and Class Members to protect their Private Information going forward, encouraging them "to remain vigilant by reviewing [their] account statements and credit reports closely."[96]

296. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

297. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[96] https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 6, 2023).

298. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[97] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

299. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

300. The retail cost of credit monitoring and identity theft monitoring typically cost in excess of $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from NextGen's Data Breach. This is a future cost that Plaintiffs and Class Members would not need to bear but for NextGen's failure to safeguard their Private Information.

CLASS ACTION ALLEGATIONS

[97]See Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

301. Plaintiffs bring this case as a class action on behalf of themselves and on behalf of a Nationwide Class ("the Class"), and on behalf of certain State Subclasses, specifically, a California Subclass, an Illinois Subclass, a New York Subclass, a Pennsylvania Subclass, a New Mexico Subclass, a New Jersey Subclass, a Maine Subclass, an Iowa Subclass and a Georgia Subclass, pursuant to Fed. R. Civ. P. 23(b)(2) and/or (b)(3), as applicable, and/or (c)(4).

302. Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

NATIONWIDE CLASS

> **All individuals residing in the United States whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendant NextGen Healthcare, Inc. provided notice to Plaintiffs and other Class Members beginning on or around April 28, 2023 (the "Nationwide Class" or "Class"), as identified by NextGen's records relating to the Data Breach.**

303. The Class asserts claims against NextGen for negligence (Count I), negligence per se (Count II), unjust enrichment (Count III), invasion of privacy/intrusion upon seclusion (Count IV), breach of implied contract (Count V), bailment (Count VI), breach of fiduciary duty (Count VII), violation of O.C.G.A. §

13-6-11 (Count VIII), violation of the Georgia Uniform Deceptive Trade Practices Act (Count IX), and declaratory judgment and injunctive relief (Count X).

304. Pursuant to Fed. R. Civ. P. 23(a), (b)(2) and/or (b)(3), as applicable, and/or (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims brought under Georgia common law. Plaintiffs also seek certification of statutory claims under state data breach statutes and consumer protection statutes (Counts XI through XXV), on behalf of separate statewide subclasses for each State identified below (the "Statewide Subclasses"), defined as follows:

305.

STATEWIDE SUBCLASSES

> **All natural persons residing in a particular state[98] whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendant NextGen Healthcare, Inc. provided notice to Plaintiffs and other Class Members beginning on or around April 28, 2023, as identified by NextGen's records relating to the Data Breach.**

306. Specifically excluded from the Nationwide Class and State Subclasses

---

[98] As described below, California, Illinois, New York, Pennsylvania, New Mexico, New Jersey, Maine, Iowa and Georgia each have a state Subclass.

are NextGen and its officers, directors, or employees; any entity in which NextGen has a controlling interest; and any affiliate, legal representative, heir, or assign of NextGen. Also excluded from the Nationwide Class and various State Subclasses are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action, as well as any individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out.

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

308. **Jurisdictional Amount.** As alleged herein, Plaintiffs seek damages on behalf of themselves and the over one million putative class members, satisfying the $5 million jurisdictional requirement of 28 U.S.C. § 1332(d)(2).

309. **Ascertainablity.** The members of the Class and State Subclasses are readily identifiable and ascertainable because the class is defined based on objective criteria. NextGen and its affiliates, among others, possess the information to identify and contact Class Members.

310. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class and State Subclasses are so numerous that joinder of all of them is

impracticable. Based on NextGen's statements, the Class contains over one million individuals whose Private Information was compromised in the Data Breach. The exact size of the Class and the identities and state citizenship of each Class Member is ascertainable from Defendants' records.

311. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Class and State Subclasses, Plaintiffs' claims are typical of the claims of the members because all Class Members had their Private Information compromised in the Data Breach and were harmed as a result. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII.

312. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs will fairly and adequately protect the interests of the Class and State Subclasses. Plaintiffs have no known interest antagonistic to those of the Class or State Subclasses and their interests are aligned with Class Members' interests. Plaintiffs were subject to the same Data Breach as Class Members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases.

313. **Commonality and Predominance: Federal Rule of Civil Procedure**

23(a)(2) and 23(b)(3). There are questions of law and fact common to the Class and State Subclasses such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class Members and will drive the resolution of this litigation. The common questions of law and fact include, without limitation:

a. Whether NextGen owed Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Private Information;

b. Whether NextGen acted negligently in connection with the collection, storage, monitoring and protection of Plaintiffs' and Class Members' Private Information;

c. Whether the Data Breach was foreseeable to NextGen given its prior ransomware attack in the same year and warnings, specifically in the Healthcare Industry, regarding the risk of data breaches;

d. Whether NextGen breached its duty to implement reasonable security systems to protect Plaintiffs' and Class Members' Private Information;

e. Whether NextGen's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

f. Whether NextGen provided timely notice of the Data Breach to Plaintiffs and Class Members;

g. Whether Plaintiffs and Class Members are entitled to compensatory damages, statutory damages, punitive damages, and/or nominal damages as a result of the Data Breach; and;

h. Whether Plaintiffs and Class Members are entitled to injunctive and declaratory relief.

314. NextGen has engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by NextGen's failure to act reasonably in collecting and storing the Private Information and to maintain reasonable security procedures and practices to protect such information, as well as NextGen's failure to timely alert affected patients to the Data Breach.

315. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** This class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. Even if Class Members had the resources to pursue individual lawsuits, the judicial system does not have the

resources to hear them. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Certifying the case as a class action will centralize millions of substantially identical claims in a single proceeding, making a class action the most manageable adjudication method for Plaintiffs, Class Members, Defendant, and the judicial system.

316. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules. NextGen acted or refused to act on grounds generally applicable to the Class by collecting, transmitting, and storing Class Members' PII without proper data security safeguards, creating actual, imminent, and ongoing threats that Class Members will experience identity theft and fraud. The common threat to each Class Member can be mitigated by NextGen's implementation of a common set of reasonable data security protocols. NextGen's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge to these policies hinges on NextGen's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

317. **Injunctive Relief is Appropriate under Federal Rule of Civil**

Procedure 23(b)(2). NextGen has failed to take actions to safeguard Plaintiffs' and Class Members' Private Information such that injunctive relief is appropriate and necessary. NextGen has acted on grounds that apply generally to the Class and State Subclasses as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis. An injunction mandating that NextGen implement appropriate protocols would constitute final injunctive relief appropriate with respect to the Class as a whole.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

318. The State of Georgia has a significant interest in regulating the conduct of businesses operating within its borders. Georgia, which seeks to protect the rights and interests of Georgia and all residents and citizens of the United States against a company headquartered and doing business in Georgia, has a greater interest in the nationwide claims of Plaintiffs and Nationwide Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

319. The principal place of business of NextGen, located at 3525 Piedmont Rd., NE, Building 6, Suite 700, Atlanta, Georgia, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy,

financial, and legal decisions. As such, NextGen's response to the Data Breach occurred in Georgia, and corporate decisions surrounding such response were made from and in Georgia.

320. NextGen's breaches of duty to Plaintiffs and Nationwide Class members emanated from Georgia.

321. Application of Georgia law to the Nationwide Class with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

322. Under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia applies to the nationwide common law claims of all Nationwide Class members. Additionally, given Georgia's significant interest in regulating the conduct of businesses operating within its borders, Georgia's Uniform Deceptive Trade Practices Act may be applied to non-resident consumer plaintiffs.

CLAIMS FOR RELIEF ON BEHALF OF THE NATIONWIDE CLASS

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

323. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

324. Plaintiffs and Class Members were required to submit their Private Information to NextGen in order to receive healthcare services from NextGen's healthcare clients.

325. In providing their Private Information, Plaintiffs and Class Members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by, cybercriminals.

326. By collecting and storing the Private Information of Plaintiffs and members of the Class on its NextGen Office system, NextGen owed to Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, NextGen was required to affirmatively design, maintain, and test its security systems to ensure that these systems were reasonably secure and capable of protecting the Private Information of Plaintiffs and the Class. NextGen further owed to Plaintiffs and the Class a duty to affirmatively implement systems and procedures that would detect a breach of its security systems in a timely manner and to timely act upon security alerts from such systems.

327. NextGen owed this duty to Plaintiffs and the other Class members because Plaintiffs and the other Class Members comprise a well-defined, foreseeable, and probable class of individuals whom NextGen should have been

aware could be injured by NextGen's inadequate security protocols.

328. NextGen actively solicited clients who entrusted NextGen with Plaintiffs' and the other Class Members' Private Information when obtaining and using NextGen's services. To facilitate these services, NextGen affirmatively used, handled, gathered, and stored the Private Information of Plaintiffs and the other Class Members. Attendant to NextGen's solicitation, use and storage, NextGen knew of its inadequate and unreasonable security practices regarding its computer/server systems and also knew that hackers and thieves routinely attempt to access, steal, and misuse the Private Information with which NextGen had been entrusted. As such, NextGen knew a breach of its systems would cause damage to Plaintiffs and the Class. Thus, NextGen had a duty to act reasonably in collecting, storing, maintaining, and protecting the Private Information of its healthcare clients' patients.

329. NextGen's duty included obligations to take reasonable steps in the management of the Private Information to prevent its disclosure and to safeguard the Private Information from theft. NextGen's duties included the responsibility to affirmatively design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

330. NextGen owed a duty of care to Plaintiffs and Class Members to

provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

331. NextGen's duty of care to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable security measures, arose as a result of the special relationship that existed between NextGen and its clients' patients, which is recognized by various laws and regulations including, but not limited to HIPAA and the FTC Act, and common law. NextGen was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

332. NextGen's duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable security measures, arose under HIPAA which required Defendant to "reasonably protect" 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)(1).

333. NextGen also had a duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable security measures, under

Section 5 of the FTC 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.

334. NextGen's duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable care in protecting such information arose not only as a result of the statutes and regulations described above, but also because NextGen is bound by industry standards to protect confidential Private Information that it either affirmatively acquires, maintains, or stores. Industry standards require NextGen to exercise reasonable care with respect to Plaintiffs and the Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, NextGen was the only entity that could adequately protect the data that that it solicited, collected, and stored.

335. NextGen's duty of care to act reasonably in collecting, storing and maintaining the Private Information, and to use reasonable care in protecting such information, arose as a result of NextGen's affirmative public representations and assurances that it would appropriately safeguard the Private Information.

336. NextGen's duty required that it safeguard the Private Information of

Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require Defendant to reasonably safeguard sensitive Private Information, as detailed herein.

337. NextGen affirmatively breached its duties to Plaintiffs and Class Members in numerous ways, as described herein, including by:

a. Acting unreasonably in collecting, storing, and maintaining the Private Information and failing to exercise reasonable care in its implementation of its security systems, protocols, and practices in order to sufficiently protect the Private Information of Plaintiffs and Class Members;

b. Negligently designing and maintaining its data security system in a manner that failed to secure Plaintiffs' and Class Members' Private Information from unauthorized access;

c. Implementing inadequate security controls;

d. Implementing inadequate security products;

e. Implementing inadequate security policies, including with respect to password protection policies and use of multi-factor authentication for its clients that use its systems;

f. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

g. Failing to test and assess the adequacy of its data security system;

h. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

i. Failing to develop and put into place uniform procedures and data security protections for its healthcare network;

j. Allocating insufficient funds and resources to the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

k. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

l. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

m. Failing to implement or update antivirus and malware protection software in need of security updating;

n. Designing its systems without encryption or without adequate encryption;

o. Designing its systems in a manner that did not require clients to use multi-factor authentication or require forced password changes; and

p. Failing to comply with its own Privacy Policy;

q. Failing to comply with regulations protecting the Private Information at issue during the period of the Data Breach;

r. Failing to recognize in a timely manner that Private Information had been compromised;

s. Waiting for a month before it disclosed the Data Breach; and

t. Otherwise negligently and affirmatively mishandling Plaintiffs' and Class Members' Private Information provided to NextGen, which in turn allowed cyberthieves to access its IT systems.

338. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze of lock their credit, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by NextGen's misconduct alleged herein.

339. NextGen is subject to an independent legal duty, untethered to any contract between it and either Plaintiffs or Class Members. The sources of NextGen's duties are alleged and described above.

340. NextGen breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information,

as alleged and described above.

341. The injuries to Plaintiffs and the other Class Members were reasonably foreseeable because NextGen knew or should have known that systems used for safeguarding Private Information were inadequately secured and exposed consumer Private Information to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, NextGen's own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class Members.

342. The injuries to Plaintiffs and the other Class Members also were reasonably foreseeable because NextGen, all persons in the healthcare and healthcare support industries, and a large portion of the public are aware of the high and ever-increasing incidence of cyberattacks perpetrated against entities in the healthcare industry, including the upward spike of cyberattacks targeted against companies in the healthcare industry during and after the COVID pandemic.

343. It was foreseeable that NextGen's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiffs and Class Members.

344. It was foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

345. The imposition of a duty of care on NextGen to safeguard the Private Information they maintained is appropriate because any social utility of NextGen's conduct is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

346. NextGen's failure to take reasonable steps to protect the Private Information of Plaintiffs and the other Class Members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiffs' and the other Class Members' Private Information. This ease of access allowed thieves to steal Private Information of Plaintiffs and the other Class Members, which has led to dissemination in black markets.

347. As a direct and proximate result of NextGen's negligence, Plaintiffs and Class Members have suffered theft of their Private Information and are at risk of ongoing and future identity theft, and Plaintiffs and Class Members sustained damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value

of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance, and nuisance, and (j) the continued imminent and future risk to their Private Information, which remains in NextGen's possession and which is subject to further breaches so long as NextGen fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

348. NextGen's conduct warrants moral blame because NextGen actively solicited its services to its clients, wherein it used, handled, and stored the Private Information of Plaintiffs and the other Class Members without disclosing that its security was inadequate and unable to protect the Private Information of Plaintiffs and the other Class Members. Holding NextGen accountable for its negligence will further the policies embodied in such law by incentivizing IT service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

349. Plaintiffs and Class Members are entitled to compensatory, consequential, and general damages suffered as a result of the Data Breach, or in the alternative, nominal damages.

350. NextGen's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

351. Plaintiffs and Class Members are also entitled to injunctive relief

requiring NextGen to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; (c) destroy the Personal Information it continues to maintain; and (d) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

352. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

353. Pursuant to the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. §§ 1320d, *et seq.*, NextGen had a duty to implement fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

354. 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 NextGen, of failing to use reasonable measures to protect Private Information. 15 U.S.C. § 45(a)(1). The FTC publications and orders described above also form part of the basis of NextGen's duty in this regard.

355. Under HIPAA, NextGen had a duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable security

measures. HIPAA required Defendant to "reasonably protect" 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)(1). HIPAA's implementing regulations, HIPAA's Security Rule, and the HHS publications described above also form part of the basis of NextGen's duty in this regard.

356. NextGen violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and failing to comply with applicable industry standards. NextGen's conduct was particularly unreasonable given the nature and amount of Private Information it obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

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

358. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA was intended to guard against. For example, 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. Further, HHS has promulgated regulations and issued specific guidance on how to protect against cybercrime.

359. NextGen's violations of Section 5 of the FTC Act and HIPAA therefore constitute negligence *per se*.

360. NextGen knew, or should have known, of the risks inherent in collecting and storing Private Information in a centralized location, NextGen's vulnerability to network attacks, and the importance of adequate security.

361. NextGen violated Section 5 of the FTC Act and HIPAA in numerous ways, as described herein, including by:

a. Acting unreasonably in collecting, storing, and maintaining the Private Information and failing to exercise reasonable care in its implementation of its security systems, protocols, and practices in order to sufficiently protect the Private Information of Plaintiffs and Class Members;

b. Negligently designing and maintaining its data security system in a manner that failed secure Plaintiffs' and Class Members' Private Information from unauthorized access;

c. Implementing inadequate security controls;

d. Implementing inadequate security products;

e. Implementing inadequate security policies, including with respect to password protection policies and use of multi-factor authentication for its clients that use its systems;

f. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

g. Failing to test and assess the adequacy of its data security system;

h. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

i. Failing to develop and put into place uniform procedures and data security protections for its healthcare network;

j. Allocating insufficient funds and resources to the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

k. Failing to ensure or otherwise require that it was compliant with applicable regulations and FTC and HHS guidelines for cybersecurity;

l. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

m. Failing to implement or update antivirus and malware protection

software in need of security updating;

n. Designing its systems without encryption or without adequate encryption;

o. Designing its systems in a manner that did not require clients to use multi-factor authentication or require forced password changes;

p. Failing to comply with its own Privacy Policy;

q. Failing to comply with regulations protecting the Private Information at issue during the period of the Data Breach;

r. Failing to recognize in a timely manner that Private Information had been compromised;

s. Waiting for a month before it disclosed the Data Breach; and

t. Otherwise negligently and affirmatively mishandling Plaintiffs' and Class Members' Private Information provided to NextGen, which in turn allowed cyberthieves to access its IT systems.

362. As a direct and proximate result of NextGen's negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the

materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued imminent and future risk to their Private Information, which remains in NextGen's possession, and which is subject to further breaches so long as NextGen fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

363. Plaintiffs and Class Members are entitled to compensatory, consequential, and general suffered as a result of the Data Breach. In the alternative, Plaintiffs are entitled to nominal damages.

364. NextGen's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

365. Plaintiffs and Class Members are also entitled to injunctive relief requiring NextGen to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; (c) destroy the Personal Information it continues to maintain; and (d) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

366. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

367. Plaintiffs and the Class Members bring this Count in the alternative to their breach of implied contract claim. Plaintiffs and Class Members have an interest, both equitable and legal, in their Private Information that was collected, stored, and maintained by NextGen and that was ultimately compromised in the Data Breach.

368. Plaintiffs and Class Members conferred a monetary benefit upon NextGen in the form of monies paid for healthcare services, a portion of which was reasonably paid for the storage and maintenance of Plaintiffs' and Class Members' Private Information in NextGen's EHR system. NextGen's business model would not exist save for the need to ensure the security of Plaintiffs' and Class Members' Private Information in order to provide its EHR and practice management solutions to its healthcare clients.

369. NextGen enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

370. The relationship between NextGen and Plaintiffs and Class Members is

not attenuated, as Plaintiffs and Class Members had a reasonable expectation that the security of their Private Information would be maintained when they provided their Private Information to NextGen's healthcare clients.

371. NextGen benefited by the conferral upon it of the Private Information pertaining to Plaintiffs and the Class Members and by its ability to retain, use, and profit from that information. NextGen understood and valued this benefit.

372. NextGen also understood and appreciated that the Private Information pertaining to Plaintiffs and Class Members was personal, private and confidential and its value depended upon NextGen maintaining the privacy and confidentiality of that Private Information.

373. Without NextGen's willingness and commitment to maintain the privacy and confidentiality of the Private Information, that Private Information would not have been transferred to and entrusted to NextGen. Further, if NextGen had disclosed that its data security measures were inadequate, it would not have been permitted to continue in operation by regulators or their clients.

374. NextGen admits that it uses the Private Information it collects for,

among other things: "marketing and promotional communications."[99]

375. Because of NextGen's collection, storage, and use of Plaintiffs' and Class Members' Private Information, NextGen sold more services and products than it otherwise would have. NextGen was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

376. NextGen also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

377. NextGen also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiffs' and Class Members' Private Information.

378. It is inequitable for NextGen to retain these benefits.

379. As a result of NextGen's wrongful conduct as alleged herein (including among other things NextGen's failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiffs

[99] https://www.nextgen.com/privacy-policy (last visited May 4, 2023).

and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that Private Information), NextGen has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

380. NextGen's unjust enrichment is traceable to and resulted directly and proximately from the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

381. It is inequitable, unfair, and unjust for NextGen to retain these wrongfully obtained benefits. NextGen's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

382. The benefit conferred upon, received, and enjoyed by NextGen was not conferred gratuitously, and it would be inequitable, unfair, and unjust for NextGen to retain the benefit.

383. NextGen's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused Plaintiffs and Class Members other damages as described herein.

384. Plaintiffs and Class Members have no adequate remedy at law.

385. NextGen is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on NextGen as a result of its wrongful conduct, including specifically: the value to NextGen of the Private Information that was stolen in the Data Breach; the profits NextGen received and is receiving from the use of that information; the amounts that NextGen overcharged Plaintiffs and Class Members for use of NextGen's products and services; and the amounts that NextGen should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT IV
Invasion of Privacy / Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Nationwide Class)

386. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

387. The State of Georgia recognizes the tort of Intrusion into Seclusion, and has adopted the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

388. NextGen required that Plaintiffs and Class Members provide Private Information to NextGen and its affiliates and Plaintiffs and Class Members wanted and expected that Private Information to remain private and non-public.

389. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure by NextGen to unauthorized parties.

390. NextGen's intentional conduct of collecting, storing, and using Plaintiffs' and Class Members' Private Information is akin to surveillance of Private Information.

391. NextGen actively participated in the intrusion into Plaintiffs' and Class Members' affairs in choosing to make inferior and inadequate data security choices that failed to protect Plaintiffs' and Class Members' Private Information and allowed unauthorized and unknown third parties to access the Private Information of Plaintiffs and Class Members.

392. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person.

393. NextGen invaded Plaintiffs' and Class Members' right to privacy and

intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

394. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members entrusted their Private Information to NextGen as a prerequisite to their use of NextGen's services, but they did so privately with the intention that their Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that their Private Information would be kept private and would not be disclosed without their authorization.

395. NextGen's inadequate data security practices and the resulting Data Breach constitute 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.

396. NextGen acted with a knowing state of mind when it permitted the Data Breach to occur because it knew or should have known that its data security practices were inadequate and insufficient.

397. Because NextGen acted with this knowing state of mind, it had notice and knew its inadequate and insufficient data security practices would cause injury

and harm to Plaintiffs and Class Members.

398. By intentionally failing to keep Plaintiffs' and Class Members' Private Information secure, and by intentionally misusing and disclosing Private Information to unauthorized parties for unauthorized use, NextGen unlawfully invaded Plaintiffs' and Class Members' privacy and right to seclusion by, inter alia:

a. Intentionally and substantially intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person;

c. Intentionally invading their privacy by improperly using their Private Information properly obtained for another purpose, or disclosing it to unauthorized persons; and

d. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

399. The Private Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other information that is the type of sensitive Private Information that one normally expects will be protected from exposure by the entity charged with

safeguarding it.

400. NextGen's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

401. NextGen's unlawful invasions of privacy damaged Plaintiffs and Class Members. As a direct and proximate result of NextGen's unlawful invasions of privacy, Plaintiffs and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

402. As a direct and proximate result of NextGen's invasion of privacy, Plaintiffs and Class Members have suffered theft of their Private Information and are at risk of ongoing and future identity theft, and Plaintiffs and Class Members sustained damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance, and nuisance; and (j) the continued imminent and future risk to their

Private Information, which remains in NextGen's possession and which is subject to further breaches so long as NextGen fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

403. Plaintiffs and Class Members are entitled to compensatory, consequential, and general damages suffered as a result of the Data Breach, or in the alternative, nominal damages.

COUNT V
Breach of Implied Contract
(*On behalf of Plaintiffs and the Nationwide Class)*

404. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

405. Plaintiffs and the Class Members entered into implied contracts with NextGen under which NextGen agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

406. NextGen acquired, stored, and maintained the Private Information of Plaintiffs and the Class that it received either directly from them or from its healthcare clients.

407. Plaintiffs and Class Members were required to provide, or authorize the transfer of, their Private Information in order for NextGen to provide its EHR

services. Plaintiffs and Class Members paid money, or money was paid on their behalf, to NextGen in exchange for services.

408. NextGen solicited, offered, and invited Class Members to provide their Private Information as part of NextGen's regular business practices. Plaintiffs and Class Members accepted NextGen's offers and provided their Private Information to NextGen.

409. NextGen accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

410. When Plaintiffs and Class Members paid money and provided their Private Information to their healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their healthcare providers and their business associates, including NextGen, and intended and understood that Private Information would be adequately safeguarded as part of that service.

411. Plaintiffs and Class Members entered into implied contracts with NextGen under which NextGen agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

412. The implied promise of confidentiality includes consideration beyond

those pre-existing general duties owed under the FTC Act, HIPAA, or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

413. The implied promises include but are not limited to: (a) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (b) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (c) restricting access to qualified and trained agents; (d) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (e) applying or requiring proper encryption; (f) multifactor authentication for access; and (g) other steps to protect against foreseeable data breaches.

414. NextGen's implied promises to safeguard Plaintiffs' and Class Members' Private information are evidenced by, *e.g.*, representations in Defendant's Privacy Policy described above.

415. Plaintiffs and the Class Members would not have entrusted their Private Information to NextGen in the absence of such an implied contract.

416. Had NextGen disclosed to Plaintiffs and the Class that it did not have

adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Private Information to NextGen.

417. NextGen recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

418. Plaintiffs and the Class Members fully performed their obligations under the implied contracts with NextGen.

419. NextGen breached the implied contract with Plaintiffs and the Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

420. As a direct and proximate result of NextGen's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages.

COUNT VI
Breach of Bailment
(On behalf of Plaintiffs and the Nationwide Class)

421. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

422. Plaintiffs' and Class Members' Private Information is personal property.

423. Plaintiffs and Class Members delivered and entrusted their Private Information to NextGen for the purpose of receiving healthcare services from their healthcare providers.

424. Plaintiffs and Class Members provided their Private Information to healthcare providers and NextGen on the express and implied conditions that they had a duty to keep the Private Information confidential.

425. In delivering their Private Information to healthcare providers and Nextgen, Plaintiffs and Class Members intended and understood that NextGen would adequately safeguard their Private Information.

426. NextGen therefore acquired and was obligated to safeguard the Private Information of Plaintiffs and Class Members.

427. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. NextGen was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

428. Once NextGen accepted Plaintiffs' and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within the

possession, custody, and control of NextGen.

429. NextGen accepted possession and took control of Plaintiffs' and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another. Accordingly, a bailment was established for the mutual benefit of the parties.

430. Specifically, a constructive bailment arises when a defendant, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

431. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously, or by mistake as to the duty or ability of the recipient to effect the purpose contemplated by the absolute owner.

432. During the bailment, NextGen owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their Private Information.

433. NextGen did not safeguard Plaintiffs' or Class Members' Private Information when failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

434. NextGen breached its duty of care by failing to take appropriate

measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to and misuse of such Private Information.

435. As a direct and proximate result of NextGen's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages.

COUNT VII
Breach of Fiduciary Duty
(*On behalf of Plaintiffs and the Nationwide Class)*

436. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

437. Plaintiffs and and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by NextGen and that was ultimately accessed or compromised in the Data Breach.

438. The Private Information of patient-Plaintiffs and Class Members was disclosed to NextGen. That Private Information is akin to the health information that was communicated to their medical providers when receiving medical care.

439. As the business associate of its healthcare clients, and recipient of

Plaintiffs' and Class Members' Private Information, NextGen has a fiduciary relationship with Plaintiffs and Class Members.

440. Because of that fiduciary relationship, NextGen was provided with and stored valuable Private Information related to Plaintiffs and Class Members. Plaintiffs and Class Members expected their information would remain confidential while in Defendant's possession.

441. In light of the special relationship between NextGen and Plaintiffs and Class Members, NextGen became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members, (a) for the safeguarding of Plaintiffs' and Class Members' Private Information; (b) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (c) to maintain complete and accurate records of what information (and where) NextGen stored that information.

442. NextGen had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its clients' patients, in particular, to keep secure their Private Information.

443. NextGen breached its fiduciary duty to Plaintiffs and Class Members by not acting reasonably in collecting, storing, and maintaining the Private Information, and in failing to encrypt the Private Information and otherwise protect

the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

444. NextGen breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

445. Plaintiffs and Class Members did not consent to nor authorize NextGen to release or disclose their Private Information to unauthorized third parties.

446. As a direct and proximate result of NextGen's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued imminent and continuing risk to their Private Information, which remains in NextGen's possession, and which is subject to further breaches so long as NextGen fails to undertake appropriate and adequate

measures to protect Plaintiffs' and Class Members' Private Information.

447. As a direct and proximate result of NextGen's breach of its fiduciary duty, Plaintiffs and Class Members are entitled to compensatory, consequential, and general damages suffered as a result of the Data Breach, or in the alternative, nominal damages.

COUNT VIII
Violation of O.C.G.A. § 13-6-11
(*On behalf of Plaintiffs and the Nationwide Class)*

448. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

449. NextGen through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs and Class Members unnecessary trouble and expense with respect to the events underlying this litigation.

450. 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 companies such as NextGen for failing to implement and use reasonable measures to protect Private Information, including PII. Further, HIPAA required Defendant to "reasonably protect" 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)(1). Various regulations and FTC and HHS publications and orders also form the basis of NextGen's duty.

451. NextGen violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with industry standards. NextGen's conduct was particularly unreasonable given the nature and amount of Private Information that it obtained and stored and the foreseeable consequences of a data breach.

452. NextGen also has a duty under the Georgia Constitution ("the Constitution") which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Constitution states "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

453. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) § 652A which specifically recognized four common law invasion of privacy claims in Georgia, which include (1) appropriation of likeness; (2) intrusion on solitude or seclusion; (3) public disclosure of private facts; and (4) false light.

454. NextGen's affirmative implementation of inadequate data security

measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiffs and Class Members to provide and stored on its own servers and databases constitutes a violation of the Constitution and the Restatement of the Law of Torts (Second).

455. NextGen knew or should have known that it had a responsibility to protect the Private Information it required Plaintiffs and Class Members to provide and stored, that it was entrusted with this Private Information, and that it was the only entity capable of adequately protecting the Private Information on its systems and data bases.

456. Despite that knowledge, NextGen abdicated its duty to protect the Private Information it required Plaintiffs and Class Members to provide and that NextGen stored.

457. As a direct and proximate result of NextGen's actions, Plaintiffs' and the Class Members' Private Information was accessed and stolen by cybercriminals. The Data Breach was a direct consequence of NextGen's abrogation of its data security responsibilities and its decision to employ knowingly deficient data security measures that knowingly left the Private Information unsecured. Had NextGen adopted reasonable data security measures, it could have prevented the Data Breach.

458. As further described above, Plaintiffs and the Class Members have been

injured and suffered losses directly attributable to the Data Breach.

459. Plaintiffs and Class Members therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

COUNT IX
Georgia Uniform Deceptive Trade Practices Act
O.C.G.A. §§ 13-1-370, *et seq.*
(*On behalf of Plaintiffs and the Nationwide Class*)

460. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

461. NextGen, Plaintiffs, and Class Members are "persons within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

462. NextGen engaged in deceptive trade practices in the conduct of its business in violation of O.C.G.A. § 10-1-372(a), which states in pertinent part that it is a deceptive trade practice to:

> (a)(5) Represent[] that goods or services have sponsorship, approval, characteristics, . . . uses, [or] benefits . . . that they do not have;
>
> (a)(7) Represent[] that goods or services are of a particular standard, quality, or grade . . . if they are of another; or

> (a)(12) Engage[] in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

463. NextGen engaged in deceptive trade practices in violation of the Georgia DTPA, Ga. Code Ann. § 10-1-372(a)(5), (7), and (12), by, among other things:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Making implied or implicit representations that its data security practices were sufficient to protect Plaintiffs' and Class Members' Private Information. NextGen made implied or implicit representations that its data security practices were sufficient to protect Plaintiffs' and Class Members' Private Information. By virtue of accepting Plaintiffs' and Class Members' Private Information from its clients, NextGen implicitly represented that its data security processes were sufficient to safeguard the Private Information;

c. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which

was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

g. Failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

464. Past breaches in the health services industry, including its own earlier in the year, put NextGen on notice that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, and NextGen knew or should have known that the risk of a data breach was highly likely.

465. Because NextGen required Plaintiffs and Class Members to provide their Private Information as a prerequisite to receive medical services from their providers, Plaintiffs and Class Members reasonably expected that Defendants' data security and data storage systems were adequately secure to protect their Private Information.

466. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

467. NextGen intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

468. Plaintiffs and Class Members relied on NextGen to advise them if their data security and data storage systems were not adequately secure to protect their Private Information.

469. Plaintiffs and Class Members had no opportunity to make any inspection of NextGen's data security practices or to otherwise ascertain the truthfulness of NextGen's representations and omissions regarding data security, including NextGen's failure to alert Plaintiffs and Class Members that their data security and data storage systems were not adequately secure and, thus, were vulnerable to attack.

470. Plaintiffs and Class Members relied to their detriment on NextGen's misrepresentations and deceptive omissions regarding their data security practices.

471. Had NextGen disclosed that its data security and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs and Class Members would not have entrusted NextGen with their Private Information.

472. NextGen acted intentionally, knowingly, and maliciously to violate the Georgia UDTPA, and recklessly disregarded Plaintiffs' and Class Members' rights. NextGen's past data breach and other industry data breaches put it on notice that its security and privacy protections were inadequate.

473. Had NextGen disclosed to Plaintiffs and Class Members that its data

systems were not secure and, thus, vulnerable to attack, NextGen would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, NextGen was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiffs the Class. NextGen accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because NextGen held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class acted reasonably in relying on NextGen's misrepresentations and omissions, the truth of which they could not have discovered.

474. As a direct and proximate result of NextGen's unfair and deceptive business practices, Plaintiffs and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the loss of value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

475. To date, NextGen has not provided sufficient details regarding the full

scope of the Data Breach, or any details related to the remedial measures it has taken to improve its data security practices and more fully safeguard Plaintiffs' and Class Members' Private Information from future compromise. As a result, Plaintiffs and Class Members remain uninformed and confused as to the adequacy of NextGen's data security and NextGen's ability to protect the Private Information entrusted to it. Without adequate improvements, Plaintiffs' and Class Members' Private Information remains at an unreasonable risk of future compromise.

476. NextGen, through its omissions and its Data Breach Notice Letters, continues to represent and imply that its data security measures are adequate to protect consumers' Private Information. Such continued representations and implications, without disclosure of the full scope of the Data Breach or NextGen's subsequent remedial enhancements, place Plaintiffs and Class Members at a future risk of harm, as Plaintiffs and Class Members are not fully informed as to whether NextGen's data security measures have been improved since the Data Breach. By all available measures, NextGen's data security practices and systems have not been adequately improved, and Plaintiffs and Class Members remain at an unreasonable risk from future cyberattacks.

477. Plaintiffs and the Class are therefore entitled to the injunctive relief sought herein, because, among other things, NextGen continues to retain their

Private Information, future cyber-attacks targeting the same data are foreseeable, and NextGen has not provided sufficient notice identifying any remedial measures that will protect the data from future attack. Moreover, absent injunctive relief, NextGen will continue to misrepresent and imply that its data security practices and systems are adequate to protect the Private Information of Plaintiffs and Class Members from future cyberattacks without providing any firm details or basis to support these representations.

478. The Georgia DTPA states that the "court, in its discretion, may award attorney's fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). NextGen willfully engaged in deceptive trade practices knowing them to be deceptive. NextGen knew or should have known that its data security practices were deficient. NextGen was aware that entities responsible for collecting and maintaining large amounts of Private Information, including Social Security numbers and financial information, are frequent targets of sophisticated cyberattacks. NextGen knew or should have known that its data security practices were insufficient to guard against those attacks.

479. The Georgia DTPA states that "[c]osts shall be allowed to the prevailing party unless the court otherwise directs." Ga. Code Ann. § 10-1-373(b). Plaintiffs

and the Class are entitled to recover their costs of pursuing this litigation.

480. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by the Georgia DTPA, including injunctive relief and attorneys' fees.

COUNT X
Declaratory and Injunctive Relief
(*On behalf of Plaintiffs and the Nationwide Class)*

481. Plaintiffs and the Class repeat and reallege by reference Paragraphs 1 through 322 above as if fully set forth herein.

482. Plaintiffs and the Class pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*.

483. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint. An actual controversy has arisen in the wake of the Data Breach regarding NextGen's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether NextGen is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent

risk that further compromises of their Private Information will occur in the future.

484. NextGen owes a duty of care to Plaintiffs and Class Members that requires it to adequately secure Plaintiffs' and Class Members' Private Information.

485. NextGen failed to fulfill its duty of care to safeguard Plaintiffs' and Class Members' Private Information.

486. As described above, actual harm has arisen in the wake of the Data Breach regarding NextGen's duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and NextGen's failure to address the security failings that led to such exposure.

487. The Court should issue prospective injunctive relief requiring NextGen to employ adequate security practices consistent with law and industry standards to protect Plaintiffs' and Class Members' Private Information.

488. NextGen still possesses the Private Information of Plaintiffs and the Class.

489. To Plaintiffs' knowledge, NextGen has not changed its data storage or security practices relating to the Private Information.

490. To Plaintiffs' knowledge, NextGen has not remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

491. To Plaintiffs' knowledge, NextGen's inadequate security practices have caused or left unremedied other vulnerabilities that may lead to additional breaches of Plaintiffs and Class Members' Private Information or personal health information.

492. NextGen had a ransomware attack and a Data Breach in the same year. The risk of another such breach is real, immediate, and substantial. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at NextGen.

493. As described above, actual harm has arisen in the wake of the Data Breach regarding NextGen's duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and NextGen's failure to address the security failings that led to such exposure.

494. There is no reason to believe that NextGen's employee training and security measures are any more adequate now than they were before the breach to meet NextGen's legal duties.

495. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to NextGen if an injunction is issued. Among other things, if another data breach occurs at NextGen, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described

herein. On the other hand, the cost to NextGen of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and NextGen has a pre-existing legal obligation to employ such measures.

496. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at NextGen, thus eliminating the additional injuries that would result to Plaintiffs and the Class.

497. Plaintiffs and Class Members, therefore, seek a declaration (1) that NextGen's existing data security measures do not comply its duties of care under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes; and (2) NextGen must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that NextGen engage internal security personnel to conduct testing, including audits on NextGen's systems, on a periodic basis, and ordering NextGen to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that NextGen engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that NextGen audit, test, and train its security personnel and

employees regarding any new or modified data security policies and procedures;

d. Ordering that NextGen purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that NextGen conduct regular database scanning and security checks;

f. Ordering that NextGen routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive Private Information, including but not limited to, client personally identifiable information.

g. Orders requiring NextGen to implement Multi-Factor Authentication and forced password changes;

h. Orders requiring NextGen to implement and install appropriate and industry standard safeguards;

i. Orders requiring NextGen to implement Multi-Factor Authentication and password protection policies, including forced password changes, for its systems and those systems used by its customers; and

j. Orders requiring NextGen to implement and install appropriate and industry standards safeguards and controls.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT XI
California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq*.

498. California Plaintiffs Alvarado and Appleton ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege Paragraphs 1 through 322, as if fully alleged herein.

499. "[T]o ensure that Private Information about California residents is protected," the California legislature enacted the California Customer Records Act, Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Private Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Private Information from unauthorized access, destruction, use, modification, or disclosure."

500. NextGen is a business that owns, maintains, and licenses "Private Information," within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiffs and California Subclass members.

501. Businesses that own, license, or maintain computerized data that

includes Private Information, including Social Security numbers, are required to notify California residents when their Private Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Private Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82. *Id.*

502. NextGen is a business that owns, licenses, or maintains computerized data that includes Private Information as defined by Cal. Civ. Code § 1798.82(h).

503. Plaintiffs and California Subclass members' Private Information includes "Private Information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

504. Because NextGen reasonably believed that Plaintiffs and California Subclass Members' Private Information was acquired by unauthorized persons during the Data Breach, NextGen had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

505. NextGen failed to disclose the Data Breach in a timely and accurate manner, within the meaning of the California Customer Records Act.

506. By failing to disclose the Data Breach in a timely and accurate manner, NextGen violated Cal. Civ. Code § 1798.82.

507. As a direct and proximate result of NextGen's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass members suffered damages, as described above.

508. Plaintiffs and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT XII
California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.

509. California Plaintiffs Alvarado and Appleton ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege Paragraphs 1 through 322, as if fully alleged herein.

510. NextGen is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

511. NextGen violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

512. NextGen's "unfair" acts and "deceptive" practices include:

a. NextGen failed to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and

theft, which was a direct and proximate cause of the Data Breach. NextGen failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents.

b. NextGen's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), HIPAA, 42 U.S.C. § 1320d, and California's Consumer Records Act (Cal. Civ. Code § 1798.81.5).

c. NextGen's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of NextGen's inadequate security, consumers could not have reasonably avoided the harms that NextGen caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

513. NextGen has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et. seq.* (requiring reasonable data security measures), California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

514. NextGen's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ.

Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*;

f. Failing to timely and adequately notify Plaintiff and California Subclass members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*

515. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

516. As a direct and proximate result of NextGen's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass Members were injured and lost money or property, including the costs passed through to NextGen, the premiums and/or price received by NextGen for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information.

517. NextGen acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass members' rights. NextGen's past data breach as well as other data breaches in the industry put it on notice that its security and privacy protections were inadequate.

518. Plaintiffs and California Subclass members seek all monetary and non-

monetary relief allowed by law, including restitution of all profits stemming from NextGen's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT XIII
California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq*. ("CLRA")

519. California Plaintiffs Alvarado and Appleton ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege Paragraphs 1 through 322, as if fully alleged herein.

520. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property, or services to consumers primarily for personal, family, or household use.

521. NextGen is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Cal. Civ. Code §§ 1761(b) and 1770. Specifically, NextGen provides EHR systems and practice management services to customers that involve storing and managing Private Information for use by

consumers and direct customers such as Defendant's healthcare clients.

522. As part of the services that NextGen offers, Defendant touts its ongoing efforts to keep consumers' Private Information secure as described above.

523. Plaintiffs and the California Class are "consumers" as defined by Cal. Civ. Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Cal. Civ. Code §§ 1761(e) and 1770.

524. NextGen engaged in unfair and deceptive acts and practices in violation of the CLRA, Cal. Civ. Code § 1770, which prohibits companies, like Defendant, from:

> (a)(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."
>
> (a)(7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (a)(14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or that are prohibited by law.

525. NextGen's acts and practices were intended to and did result in the sale of services to Plaintiffs Alvarado and Appleton and California Subclass Members in violation of the CLRA, Cal. Civ. Code § 1770(a)(5), (7) and (14), by, among other things, omitting and concealing the material fact that NextGen did not implement

and maintain adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information.

526. NextGen's acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass members in violation of Cal. Civ. Code § 1770's, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised;

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not;

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which

was a direct and proximate cause of the Data Breach;

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d, and common law, which was a direct and proximate cause of the Data Breach;

h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

j. Failing to timely and adequately notify Plaintiffs and California Subclass Members of the Data Breach;

k. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass Members' Private Information; and

l. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

527. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

528. Had NextGen disclosed to Plaintiffs Alvarado and Appleton and California Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NextGen would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, NextGen was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiffs the California Subclass. NextGen accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because NextGen held itself out as maintaining a secure platform for Private Information data, Plaintiffs and the California Subclass acted reasonably in relying on NextGen's misrepresentations and omissions, the truth of which they could not have discovered.

529. As a direct and proximate result of NextGen's violations of Cal. Civ. Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

530. Plaintiffs and the California Subclass have provided notice of their claims for damages to NextGen, on November 10, 2023, in compliance with Cal. Civ. Code § 1782(a). NextGen failed to cure the deficiencies that led to the Data Breach and the harm caused to Plaintiffs Alvarado and Appleton and the California Subclass.

531. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT XIV
California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, *et seq.*

532. The California Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege

Paragraphs 1 through 322, as if fully alleged herein.

533. California Plaintiffs Alvarado and Appleton bring this claim individually and on behalf of the California Subclass against NextGen for violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA").

534. Plaintiffs Alvarado and Appleton and California Subclass Members are consumers and California residents as defined by Cal. Civ. Code §1798.140(i).

535. NextGen is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over $25 million.

536. NextGen is a business that collects consumers' Private Information as defined by Cal. Civ. Code § 1798.140(e). Specifically, NextGen obtains, receives, or accesses consumers' Private Information when customers use NextGen's products to maintain and process consumer data.

537. NextGen and its direct customers determine the purposes and means of processing consumers' Private Information. NextGen uses consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test Nextgen's services.

538. NextGen had a duty to implement and maintain reasonable data security

procedures and practices to protect Plaintiffs Alvarado's and Appleton's and California Subclass Members' Private Information. As a direct and proximate result of NextGen's violations of its to implement and maintain reasonable security procedures and practices, Plaintiffs Alvarado's and Appleton's and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft and/or disclosure in violation of the CCPA, Cal. Civ. Code § 1798.150.

539. NextGen violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs' and the California Subclass Members' nonencrypted and nonredacted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Nextgen's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

540. NextGen knew or should have known that its data security practices were inadequate to secure California Subclass Members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

541. NextGen failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

542. NextGen stored and maintained Plaintiffs Alvarado and Appleton and California Subclass Members' Private Information in a form that allowed criminals to access it.

543. The cybercriminals accessed "nonencrypted and unredacted Private Information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

544. NextGen violated the CCPA, Cal. Civ. Code § l798.150(a), by failing to prevent Plaintiff Alvarado's and Appleton's and California Subclass Members' Private Information from unauthorized access and exfiltration, theft, or disclosure.

545. Because NextGen is still in possession of Plaintiff Alvarado's and Appleton's and California Subclass Members' Private Information, Plaintiffs and the California Subclass seek injunctive or other equitable relief to ensure that NextGen implements and maintains reasonable data security measures and practices to prevent an event like the Data Breach from occurring again.

546. Plaintiff seeks injunctive relief in the form of an order requiring NextGen to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' Private Information, requiring NextGen to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass Members' authorization,

along with an explanation of how the data breach occurred.

547. Plaintiff and the California Subclass Members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civ. Code § 1798.150(a)(1)(A).

548. As a direct and proximate result of NextGen's violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

549. On November 10, 2023, NextGen was sent written notice of its violations of Cal. Civ. Code § 1798.150(a) and the notice further demanded that such violations be cured, pursuant to Cal. Civ. Code § 1798.150(b). Because NextGen has neither cured the noticed violation nor provided Plaintiff with an express written statement that the violations have been cured and that no further violations shall occur, Plaintiff and the California Subclass seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

550. NextGen has failed to cure the violations of the CCPA. Plaintiffs Alvarado and Appleton and the California Subclass therefore seek all actual and compensatory damages according to proof or statutory damages allowable under the CCPA, whichever are higher, and such other and further relief as this Court may deem just and proper, including injunctive or declaratory relief.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT XV
Illinois Personal Information Protection Act
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

551. Illinois Plaintiff Bailey identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

552. As a publicly held corporation which handled, collected, disseminated, and otherwise dealt with nonpublic Private Information, NextGen was a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

553. Plaintiff and Illinois Subclass members' Private Information (*e.g.*, Social Security numbers) includes personal information as covered under 815 Ill. Comp. Stat. § 530/5.

554. As a Data Collector, NextGen was required to notify Plaintiff and Illinois Subclass members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

555. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, NextGen violated 815 Ill. Comp. Stat. §

530/10(a).

556. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

557. As a direct and proximate result of NextGen's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass members suffered damages, as described above.

558. Plaintiff and Illinois Subclass members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of NextGen's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT XVI
Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp. Stat. §§ 505, *et seq*. (Illinois CPA")

559. Illinois Plaintiff Bailey ("Plaintiff" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

560. Plaintiff Bailey brings this claim, individually and on behalf of the Illinois Subclass, against NextGen for violations of the Illinois Consumer Fraud and

Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505, *et seq.* ("Illinois CPA").

561. NextGen is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

562. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

563. NextGen's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

564. NextGen's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members'

Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Illinois Class Members of the Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

565. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

566. NextGen intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions. Plaintiffs and

Illinois Subclass Members reasonably relied on NextGen to advise them if their data security and data storage systems were not adequately secure to protect their Private Information, the truth of which they could not otherwise have discovered.

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

568. NextGen acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights. NextGen's past data breach as well as other industry breaches put it on notice that its security and privacy protections were inadequate.

569. As a direct and proximate result of NextGen's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

570. Plaintiff and Illinois Subclass Members seek all monetary and non-

monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XVII
Illinois Uniform Deceptive Trade Practices Act
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

571. Illinois Plaintiff Bailey ("Plaintiff" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

572. NextGen is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

573. NextGen engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

574. NextGen's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' Private Information, including by implementing and maintaining reasonable security

measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Illinois Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and

Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

575. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

576. The above unfair and deceptive practices and acts by NextGen were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

577. As a direct and proximate result of NextGen's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

578. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT XVIII

Private Information Security Breach Protection Law Iowa Code § 715C.2

579. Iowa Plaintiff Kerr ("Plaintiff" for purposes of this Count), individually, on behalf of J.K., and behalf of the Iowa Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

580. NextGen is a business that owns or licenses computerized data that includes "Private Information" as defined by Iowa Code § 715C.2(1).

581. Plaintiff and Iowa Subclass Members' Private Information includes "Private Information" as covered under Iowa Code § 715C.2(1).

582. NextGen is required to accurately notify Plaintiff and Iowa Subclass Members if it becomes aware of a breach of its data security program in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

583. Because NextGen was aware of a breach of its security system, NextGen had an obligation to disclose the data breach in a timely and accurate

fashion as mandated by Iowa Code § 715C.2(1).

584. NextGen failed to disclose the data breach in a timely and accurate manner, within the meaning of Iowa Code § 715C.2(1).

585. By failing to disclose the Data Breach in a timely and accurate manner, NextGen violated Iowa Code § 715C.2(1).

586. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

587. As a direct and proximate result NextGen's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass Members suffered damages, as described above.

CLAIMS ON BEHALF OF THE MAINE SUBCLASS

COUNT XIX
Maine Unfair Trade Practices Act
5 Me. Rev. Stat. §§205, 213, *et seq.*

588. Maine Plaintiff Miller ("Plaintiff" for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

589. NextGen is a "person" as defined by 5 Me. Stat. § 206(2).

590. NextGen's conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

591. Plaintiff and Maine Subclass Members purchased goods and/or services for personal, family, and/or household purposes.

592. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) on November 10, 2023.

593. NextGen engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Maine Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of

Plaintiff's and Maine Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maine Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify the Plaintiff and Maine Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

594. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

595. Had NextGen disclosed to Plaintiff and Maine Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NextGen would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, NextGen was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiff the Maine Subclass. NextGen accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because NextGen held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Maine Subclass acted reasonably in relying on NextGen's misrepresentations and omissions, the truth of which they could not have discovered.

596. As a direct and proximate result of NextGen's unfair and deceptive acts and conduct, Plaintiff and Maine Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

597. Plaintiff and the Maine Subclass Members seek all monetary and non-

monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

COUNT XX
Maine Uniform Deceptive Trade Practices Act
10 Me. Rev. Stat. §§ 1212, *et seq*.

598. Maine Plaintiff Miller ("Plaintiff" for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

599. NextGen is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

600. NextGen advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

601. NextGen engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or

misunderstanding.

602. NextGen's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Maine Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Maine Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maine

Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify the Plaintiff and Maine Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

603. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

604. NextGen intended to mislead Plaintiff and Maine Subclass Members and induce them to rely on its misrepresentations and omissions.

605. Had NextGen disclosed to Plaintiff and Maine Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NextGen would have

been unable to continue in business and it would have beenforced to adopt reasonable data security measures and comply with the law. Instead, NextGen was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiff and the Maine Subclass. NextGen accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because NextGen held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Maine Subclass acted reasonably in relying on NextGen's misrepresentations and omissions, the truth of which they could not have discovered.

606. As a direct and proximate result of NextGen's deceptive trade practices, Plaintiff and Maine Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

607. Maine Subclass members are likely to be damaged by NextGen's ongoing deceptive trade practices.

608. Plaintiff and the Maine Subclass Members seek all monetary and non-monetary relief allowed by law, including damages or restitution,injunctive or other

equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT XXI
New Jersey Customer Security Breach Disclosure Act, N.J. Stat. Ann. §§ 56:8-163, *et seq*.

609. New Jersey Plaintiffs Akhras, Alturi, and Phillips ("Plaintiffs" for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

610. NextGen is a business that compiles or maintains computerized records that include Private Information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

611. Plaintiffs' and New Jersey Subclass Members' Private Information (including names, addresses, and Social Security numbers) includes Private Information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

612. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Private Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Private Information was, or is reasonably believed to have been, accessed by an unauthorized person."

613. Because NextGen discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, NextGen had an obligation to disclose the Data Breach in a timely and accurate fashion.

614. NextGen failed to disclose the Data Breach in a timely and accurate fashion, within the meaning of N.J. Stat. Ann. §§ 56:8-163, *et. seq.*

615. By willfully, knowingly, and/or recklessly failing to disclose the Data Breach in a timely and accurate manner, NextGen violated N.J. Stat. Ann. § 56:8-163(b).

616. As a direct and proximate result of NextGen's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiffs and New Jersey Subclass Members suffered the damages described above.

617. Plaintiffs and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT XXII
New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1, *et seq*.

618. New Jersey Plaintiffs Akhras, Alturi, and Phillips ("Plaintiffs" for purposes of this Count), individually and on behalf of the New Jersey Subclass,

repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

619. NextGen is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

620. NextGen sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

621. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

622. NextGen's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and New Jersey Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to

the security and privacy of Plaintiffs' and New Jersey Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify Plaintiffs and New Jersey Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security

and privacy of Plaintiffs and New Jersey Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

623. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

624. NextGen intended to mislead Plaintiffs and New Jersey Subclass Members and induce them to rely on its misrepresentations and omissions. Plaintiffs and New Jersey Subclass Members reasonably relied on NextGen to advise them if their data security and data storage systems were not adequately secure to protect their Private Information, the truth of which they could not otherwise have discovered.

625. NextGen acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and New Jersey Subclass Members' rights. NextGen's past data breach and other industry data breaches put it on notice that its security and privacy protections were inadequate.

626. As a direct and proximate result of NextGen's unconscionable and deceptive practices, Plaintiffs and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and

monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

627. Plaintiffs and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS

COUNT XXIII

New Mexico Unfair Practices Act
N.M. Stat. Ann. §§ 57-12-2, *et seq.*

628. New Mexico Plaintiff Bundy ("Plaintiff" for purposes of this Count), individually, on behalf of for A.B., and on behalf of the New Mexico Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

629. NextGen is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

630. NextGen was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

631. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, et

seq., prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

632. NextGen engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

a. Knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5);

b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7);

c. Knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14);

d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff and the New Mexico Subclass' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico

Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

633. NextGen's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New Mexico Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Mexico Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and New Mexico statutes requiring protections for Social Security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New Mexico Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Mexico Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Failing to timely and adequately notify Plaintiff and New Mexico Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New Mexico Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4.

634. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

635. NextGen intended to mislead Plaintiff and New Mexico Subclass Members and induce them to rely on its misrepresentations and omissions. Plaintiffs and New Mexico Subclass Members reasonably relied on NextGen to advise them if their data security and data storage systems were not adequately secure to protect their Private Information, the truth of which they could not otherwise have discovered.

636. NextGen acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass members' rights.

637. As a direct and proximate result of NextGen's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass Members have

suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

638. Plaintiff and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT XXIV
New York General Business Law
N.Y. Gen. Bus. Law §§ 349, *et seq.*

639. New York Plaintiff Benn ("Plaintiff" for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

640. NextGen engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy

measures to protect Plaintiff's and New York Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting to those obtaining medical treatment in New York that it would protect the privacy and confidentiality of Plaintiffs and New York Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting to those obtaining medical treatment in New York that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass Members' Private Information, including duties imposed by the by FTC Act, 15

U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify Plaintiff and New York Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

641. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

642. NextGen acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights.

643. As a direct and proximate result of NextGen's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will

continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

644. NextGen's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

645. The above deceptive and unlawful practices and acts by NextGen caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

646. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT XXV
Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.

647. Pennsylvania Plaintiff Brickle ("Plaintiff" for purposes of this Count),

individually and on behalf of the Pennsylvania Subclass, repeats and alleges Paragraphs 1 through 322, as if fully alleged herein.

648. NextGen is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

649. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

650. NextGen engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

651. NextGen's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass members'

Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Pennsylvania Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify Plaintiff and Pennsylvania

Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Pennsylvania Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1320d.

652. NextGen's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NextGen's data security and ability to protect the confidentiality of consumers' Private Information.

653. NextGen intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

654. Had NextGen disclosed to Plaintiffs, Class members, and its customers that its data systems were not secure and, thus, vulnerable to attack, NextGen would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, NextGen held itself out as one of the leading electronic medical record companies, and NextGen

was trusted with sensitive and valuable Private Information regarding millions of patients, including Plaintiff and the Pennsylvania Subclass. NextGen accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because NextGen held itself out as having a special role in the healthcare system with a corresponding duty of trustworthiness and care, Plaintiff and the Pennsylvania Subclass members acted reasonably in relying on NextGen's misrepresentations and omissions, the truth of which they could not have discovered.

655. NextGen acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights. NextGen's past data breaches, as well as other healthcare industry data breaches put it on notice that its security and privacy protections were inadequate.

656. As a direct and proximate result of NextGen's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts

for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

657. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs and their Counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit and prevent NextGen from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by NextGen as a result of their unlawful

acts, omissions, and practices;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses under O.C.G.A. Section 13-6-11 and as otherwise allowed by law; and

F. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: December 11, 2023

/s/ MaryBeth v. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Tel.: 404-978-6971
Fax: 404-320-9978
mgibson@thefinleyfirm.com

/s/ J. Cameron Tribble
Roy E. Barnes
Georgia Bar No. 03900
J. Cameron Tribble
Georgia Bar No. 754759
Kristen Tullos Oliver
Georgia Bar No. 941093

BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Telephone: 770-227-6375
Fax: 770-227-6373
E-Mail: roy@barneslawgroup.com
E-Mail: ctribble@barneslawgroup.com
E-Mail: ktullos@barneslawgroup.com

/s/ Norman. E. Siegel
Norman E. Siegel,* Missouri Bar No. 44378
Jillian R. Dent,* Missouri Bar No. 68716
Tanner J. Edwards,* Missouri Bar No 68039
Brandi S. Spates,* Missouri Bar No 72144
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
dent@stuevesiegel.com
tanner@stuevesiegel.com
spates@stuevesiegel.com

Interim Co-Lead Counsel for Plaintiffs
** Pro Hac Vice*