

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF KINGS**

LISA SIMMONS and KELLY PETERSON-
SMALL, *individually and on behalf of all others
similarly situated,*

Plaintiffs,

v.

ASSISTCARE HOME HEALTH SERVICES
LLC,
d/b/a Preferred Home Care of New
York/Preferred Gold,

Defendant.

Index No. _____

**CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Lisa Simmons and Kelly Peterson-Small (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this action against Defendant Assistcare Home Health Services LLC, a New York limited liability company that does business as Preferred Home Care of New York/Preferred Gold (“Preferred Home” or “Defendant”), to obtain damages, restitution, and injunctive relief from Defendant for the Class, as defined below. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach (“Data Breach”) at Preferred Home, a home-care provider that offers home health services throughout central New York. As a result of the Data Breach, Plaintiffs and approximately 92,283 Class

Members¹ suffered ascertainable losses in the form of the imminent risk of future harm from the theft of their Social Security numbers and other private information, the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the cyberattack.

2. In addition, Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, demographic information, Social Security numbers, addresses, email addresses, phone numbers, dates of birth, bank account numbers, and medical information such as health assessments, physicals, drug screens, vaccinations, TB tests, FMLA and workers compensation claims, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and additional personally identifiable information (“PII”) and protected health information (“PHI”) that Defendant collected and maintained (collectively the “Private Information”).

4. Plaintiffs bring this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a reckless manner.

6. In particular, the Private Information was maintained on Defendant's computer

¹ See *Data Breach Notifications*, Office of the Main Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/3d7936dd-8f7d-4148-bae8-adcc722c1486.shtml> (last visited Apr. 20, 2021).

network in a condition vulnerable to cyberattacks, such as the cyberattack that enabled third-party cyber-thieves to access a file on Defendant's network.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures

to deter and detect identity theft.

13. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Preferred Home's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

15. Plaintiff Lisa Simmons is, and at all times mentioned herein was, an individual citizen of the State of New York residing in New York County. Plaintiff worked as a Personal Assistant for Preferred Home between October 2018 and November 2019. Plaintiff was notified of Defendant's Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated March 10, 2021.²

16. Plaintiff Kelly Peterson-Small is, and at all times mentioned herein was, an individual citizen of the State of New York residing in Kings County. Plaintiff worked as an RN Coordinator for Preferred Home between approximately 2016 and August 2019. Plaintiff was notified of Defendant's Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated March 10, 2021.³

17. Defendant Assistcare Home Health Services LLC, doing business as Preferred Home Care of New York/Preferred Gold, is a New York limited liability company that offers home health services throughout New York with its principal place of business at 2357 60th Street,

² See Exhibit A.

³ See Exhibit B.

Brooklyn, New York 11204.

JURISDICTION AND VENUE

18. This Court has jurisdiction over Defendant and Plaintiffs' claims under CPLR § 301 and 302(a) because Preferred Home (i) is a New York limited liability corporation with its principal place of business in New York, (ii) committed tortious acts in New York, and (iii) has sufficient minimum contacts and engaged in significant business activity in the State of New York.

19. Venue is proper in Kings County pursuant to CPLR § 503 because Defendant Preferred Home is headquartered in and does business in this County, the cause of action accrued in this county, and Preferred Home has an office for the transaction of its customary business in this County.

DEFENDANT'S BUSINESS

20. Defendant Preferred Home, founded in 2007, provides home-health services in 14 New York counties.⁴

21. Preferred Home provides in-home nursing services and specialty care⁵ and aides⁶ that provide medical care and help with daily tasks for individuals suffering from stroke, diabetes, Alzheimer's, cancer, and Parkinson's.

22. Since its founding in 2007, Preferred Home claims to have provided services to 40,000 families and be among the largest licensed home-care agency in the New York Metropolitan area.⁷

⁴ *Service Areas*, Preferred Home Care of New York, <https://preferredhcnyc.com/service-areas/> (last visited Apr. 22, 2021).

⁵ *See Nursing Services*, Preferred Home Care of New York, <https://preferredhcnyc.com/nursing-services/> (last visited Apr. 22, 2021).

⁶ *See In-Home Aides*, Preferred Home Care of New York, <https://preferredhcnyc.com/homeaides/> (last visited Apr. 22, 2021).

⁷ *See Homepage*, Preferred Home Care of New York, <https://preferredhcnyc.com/> (last visited Apr. 22, 2021).

23. As of 2021, Defendant Preferred Home states that it has 9 office locations and maintains a workforce of 250 “on-site coordinators and case managers” and 7,000 aides throughout 14 counties in New York State.⁸

24. On information and belief, in the ordinary course of rendering in-home healthcare services, Preferred Home requires employees and consumers to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Demographic information;
- Financial account information, such as a bank account number;
- Health assessments;
- Medical histories;
- Drug screens and medication or prescription information;
- Vaccination history;
- TB test history, and;
- Address, phone number, and email address, and;

25. On information and belief, as a condition of employment, Preferred Home collects and maintains the above personal, health, and financial information about its employees. Also, Preferred Home obtains Personal Information and employment data within the context of a person’s working relationship with Preferred Home. Such persons include, for example, job applicants, employees (whether temporary or permanent), contingent workers, retirees, and former

⁸ *Id.*

employees, as well as any dependents or beneficiaries.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant 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.

27. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

28. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE CYBER-ATTACK AND DATA BREACH

29. On January 9, 2021, Defendant "identified a disruption on its network[.]"⁹

30. Defendant, via a third-party, launched an investigation into this disruption event and determined that an unauthorized third-party gained access to Preferred Home's network.¹⁰

31. According to Defendants investigation, between January 8, 2021 and January 10, 2021, an unauthorized third-party was able to gain access to Defendant's sensitive files containing protected and confidential Private Information on Defendant's network.¹¹

32. Upon information and belief, the cyberattack was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

33. Upon information and belief, the targeted cyberattack was expressly designed to

⁹ See *Assistcare Home Health Services LLC dba Preferred Home Care of New York/Preferred Gold Notified Individuals of Privacy Incident*, Preferred Home Care of New York, <https://preferredhcnyc.com/wp-content/uploads/2021/03/Web-notice.pdf> (last visited Apr. 23, 2021).

¹⁰ *Id.*

¹¹ *Id.*

gain access to private and confidential data, including (among other things) the PII and PHI of patients, employees and former employees, like Plaintiffs and the Class Members.

34. Because of this targeted cyberattack, data thieves were able to gain access to Defendant's computer network and subsequently access the protected Private Information of Plaintiffs and Class Members.

35. By Defendant's own admission, the hackers and unauthorized third-party were even potentially able to "acquire some individuals' personal information on its network" which means that Plaintiffs' and Class Members Private Information was likely exfiltrated as well, not merely viewed without authorization.¹²

36. The file accessed by this incident contained the following information: names, demographic information, Social Security numbers, addresses, email addresses, phone numbers, dates of birth, bank account numbers, and medical information such as health assessments, physicals, drug screens, vaccinations, TB tests, FMLA and workers compensation claims, and other protected health information.¹³

37. The Private Information contained in the file was not encrypted.

38. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs further believe their stolen Private Information was subsequently sold on the Dark Web.

39. Unsurprisingly, Preferred Home could not rule out that Private Information was viewed or accessed in the Data Breach.¹⁴ In fact, Defendant confirmed Private Information was viewed and likely exfiltrated.¹⁵

40. Defendant's offer of identity monitoring services is an acknowledgment by

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

Preferred Home that the impacted current and former employees are subject to an imminent threat of fraud and identity theft.

41. Despite the Data Breach occurring on January 9, 2021 and acknowledging that data thieves likely accessed Plaintiffs' and the Class Members' Private Information, Defendant did not begin to notify affected individuals until March 10, 2021, about 2 months later.¹⁶

42. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

43. In addition, Defendant had obligations created by HIPAA, state law, and its own promises and representations to promptly notify impacted individuals of the Data Breach.

44. Plaintiffs and Class Members provided their Private Information to Preferred Home with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

45. Preferred Home's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

46. In light of recent high profile data breaches at other healthcare partner and provider companies, including (by way of example) American Medical Collection Agency (25 million individuals, March 2019) University of Washington Medicine (974,000 individuals, December 2018), Florida Orthopedic Institute (640,000 individuals, July 2020), Wolverine Solutions Group (600,000 individuals, September 2018), Oregon Department of Human Services (645,000

¹⁶ *Id.*

individuals, March 2019), Elite Emergency Physicians (550,000 individuals, June 2020), Magellan Health (365,000 individuals, April 2020), BJC Health System (286,876 individuals, March 2020), Preferred Home knew or should have known that its electronic records would be targeted by cybercriminals

47. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential healthcare targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁷

48. In fact, according to the cybersecurity firm Mimecast, “90% of healthcare organizations experienced email-borne attacks in the past year[.]”¹⁸

49. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Preferred Home’s industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

50. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly

¹⁷ *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Apr. 27, 2021).

¹⁸ See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁹ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁰

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

¹⁹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 26, 2021).

²⁰ *Id.*

Section 5 of the FTC Act.”)

55. Defendant failed to properly implement basic data security practices.

56. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to current and former employees PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

57. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its current and former employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

58. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyber-attacks because of the value of the PII and PHI they collect and maintain.

59. Healthcare industry experts assert that “data breaches cost the healthcare industry approximately \$5.6 billion every year[.]”

60. According to the University of Illinois Chicago (UIC), “[t]o improve cybersecurity in healthcare, organizations need to hire informatics professionals who can not only collect, manage and leverage data, but protect it as well.”²¹

61. UIC has identified several strategies and best practices that, at a minimum, should be implemented by healthcare providers like Defendant, including but not limited to: establishing a security culture; protecting mobile devices; thoroughly educating all employees; strong passwords that need to be changed regularly; multi-layer security, including firewalls, anti-virus,

²¹ See *Cybersecurity: How Can It Be Improved in Health Care?*, Health Informatics-University of Illinois Chicago, July 13, 2020, <https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/> (last visited Apr. 27, 2021).

and anti-malware software; limiting network access; controlling physical access to devices; encryption; making data unreadable without a password or key; multi-factor authentication; backup data; and limiting employees access to sensitive and protected data.²²

62. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security (CIS) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these guidelines.²³

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

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

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

65. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive current and former employees' health information.

²² *Id.*

²³ *CIS Benchmarks™ FAQ*, Center for Internet Security, <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/> (last visited Apr. 27, 2021).

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

67. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PII like the data Preferred Home left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

68. Cyberattacks such as the one Preferred Home experienced are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See* 45 C.F.R. 164.40

69. Preferred Home’s Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT’S BREACH

70. Preferred Home breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Preferred Home’s unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect current and former employees' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- h. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- i. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

- k. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
 - l. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR § 164.304’s definition of “encryption”);
 - m. Failing to notify Plaintiffs and Class Members of the Data Breach promptly;
 - n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
 - o. Failing to adhere to industry standards for cybersecurity.
71. Preferred Home negligently and unlawfully failed to safeguard Plaintiffs’ and Class Members’ Private Information.
72. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Preferred Home.

Cyberattacks and Data Breaches Put Consumers at an Increased Risk of Fraud and Identity Theft

73. Cyberattacks and data breaches at medical facilities like Preferred Home are especially problematic because of the increased risk of fraud and identity theft that arise therefrom.
74. The United States Government Accountability Office released a report in 2007

regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁴

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims’ identities in order to engage in illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity, or otherwise harass or track the victim.

76. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number.

77. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

78. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 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.²⁵

²⁴ See U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at <https://www.gao.gov/new.items/d07737.pdf>.

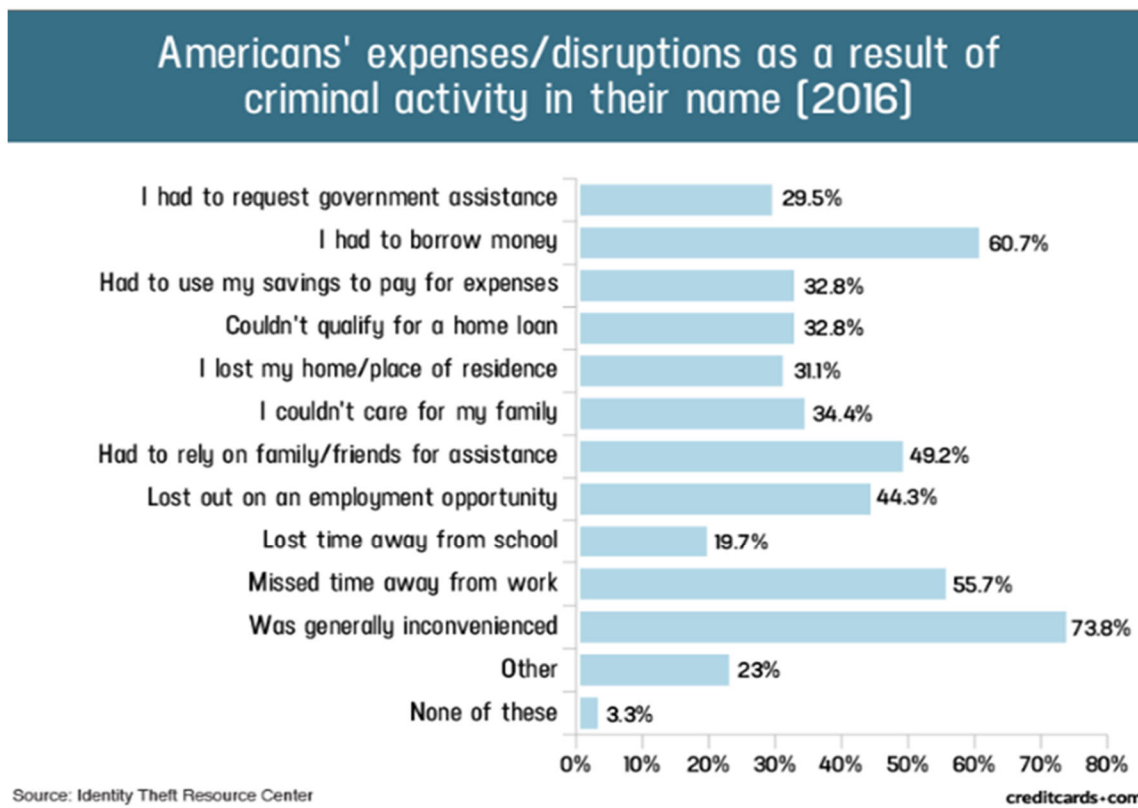
²⁵ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited Apr 1, 2021).

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

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

81. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:²⁶

²⁶ See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>.



82. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.²⁷

83. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

84. Theft of PHI, in particular, is gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment,

²⁷ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

insurance and payment records, and credit report may be affected.”²⁸

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

86. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

87. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

88. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

89. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

²⁸ *See* Federal Trade Commission, *Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Apr. 28, 2021).

90. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

91. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.²⁹ PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

92. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.³⁰ Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.³¹ Each of these fraudulent activities is difficult to detect. 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.

93. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

94. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security

²⁹ 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/>.

³⁰ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Apr. 28, 2021).

³¹ *Id.* at 4.

number.”³²

95. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”³³

96. Medical information is especially valuable to identity thieves. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries. For this reason, Preferred Home knew or should have known about these dangers and strengthened its network security and data handling systems accordingly.

97. Preferred Home was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiffs’ and Class Members’ Damages

98. To date, Defendant has done virtually nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

99. The complimentary fraud and identity monitoring service offered by Preferred Home is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

100. Plaintiffs and Class Members have been damaged by the compromise of their

³² Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

³³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

Private Information in the Data Breach.

101. As a result of the Data Breach, Plaintiff Lisa Simmons believes that a claim for unemployment insurance benefits was fraudulently filed using her identity. Plaintiff Simmons was forced to expend approximately four hours to address this fraudulent claim, including contacting the New York Department of Labor to dispute the claim. Moreover, the false claim affected Plaintiff Simmons' ability to claim unemployment benefits for herself.

102. Since January of 2021, the month the Data Breach occurred, Plaintiff Simmons has experienced a substantial increase in scam phone calls and emails. Plaintiff Simmons receives approximately six scam phone calls and five scam emails each day, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

103. As a result of the Data Breach, Plaintiff Kelly Peterson-Small has experienced multiple unauthorized and fraudulent charges to her TD Bank debit card. Starting in February of 2021, Plaintiff Peterson-Small suffered fraudulent charges from Apple, PC Richard & Son, and Western Union. Due to these unauthorized charges, Plaintiff Peterson-Small filed disputes with TD Bank over these charges and had to get a replacement debit card three times. Plaintiff Peterson-Small was forced to expend approximately six hours to address these unauthorized and fraudulent charges.

104. Since January of 2021, the month the Data Breach occurred, Plaintiff Peterson-Small has experienced a substantial increase in scam phone calls and emails. Each day, Plaintiff Peterson-Small receives approximately two scam phone calls and ten scam emails, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

105. Simply put, Plaintiffs' and Class Members' PII and PHI were compromised as a direct and proximate result of the Data Breach.

106. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

107. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

108. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

109. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

110. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

111. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

112. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about

all the time that they will need to spend monitor their own accounts, or to establish a “security freeze” on their credit report.³⁴

113. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges, insurance claims, and/or government benefit claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with credit reporting agencies;
- d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;
- e. Contacting financial institutions and closing or modifying financial accounts;
- f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

114. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

³⁴ See *Preferred Home Template Notice Letter*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/3d7936dd-8f7d-4148-bac8-adcc722c1486/7167a634-1180-4708-be7d-715cf42ab7c8/document.html> (last visited Apr. 29, 2021).

115. As a direct and proximate result of Preferred Home's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

116. Pursuant to New York's Civil Practice Law and Rules (C.P.L.R.) Section 901(a), Plaintiffs seek certification of the following class of persons defined as follows:

All persons Preferred Home identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the Class are any judges presiding over this matter and court personnel assigned to this case.

117. **Numerosity (C.P.L.R. § 901(a)(1)).** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, the Class reportedly include approximately 92,283 people. The identities of Class Members are ascertainable through Preferred Home's records, Class Members' records, publication notice, self-identification, and other means.

118. **Commonality (C.P.L.R. § 901(a)(2)).** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Preferred Home unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether Preferred Home failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyberattack and Data Breach;

- c. Whether Preferred Home's data security systems prior to and during the cyberattack and Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;
- d. Whether Preferred Home's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Preferred Home owed a duty to Class Members to safeguard their Private Information;
- f. Whether Preferred Home breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers and data thieves obtained Class Members' Private Information in the Data Breach;
- h. Whether Preferred Home knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Preferred Home owed a duty to provide Plaintiffs and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;
- j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Preferred Home's misconduct;
- k. Whether Preferred Home's conduct was negligent;
- l. Whether Preferred Home's conduct violated federal law;
- m. Whether Preferred Home's conduct violated state law;
- n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

119. Common sources of evidence may also be used to demonstrate Preferred Home's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Preferred Home's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

120. **Typicality (C.P.L.R. § 901(a)(3)).** Plaintiffs' claims are typical of the claims of the Class they seek to represent, in that the named Plaintiffs and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests adverse to the interests of the other members of the Class.

121. **Adequacy of Representation (C.P.L.R. § 901(a)(4)).** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

122. **Predominance (C.P.L.R. § 901(a)(2)).** Preferred Home has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

123. **Superiority (C.P.L.R. § 901(a)(5)).** A 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 Class Members would likely find that the cost of litigating their individual

claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Preferred Home. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

124. Preferred Home has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

125. Certification is appropriate because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Preferred Home owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- b. Whether Preferred Home's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Preferred Home's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Preferred Home failed to take commercially reasonable steps to safeguard consumer Private Information; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

126. Finally, all members of the proposed Class are readily ascertainable. Preferred Home has identified those persons whose information was contained in the file accessed by unauthorized persons and has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Preferred Home.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

(On Behalf of Plaintiffs and the Class)

127. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-126 as if fully set forth herein.

128. In order to gain employment with Defendant, Preferred Home employee Class Members to submit non-public Private Information, such as PII and PHI. Similarly, in order to receive medical treatments and services, Preferred Home required patient Class Members to submit non-public Private Information, such as PII and PHI.

129. Plaintiffs and Class Members entrusted their Private Information to Preferred Home with the understanding that Preferred Home would safeguard their information.

130. By collecting and storing this data in its computer property, Defendant had, and continues to have, a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

131. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of employment with the company and/or to obtain treatment from Defendant. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the Class Members from a data breach.

132. Defendant 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, and the personnel responsible for them, adequately protected the Private Information.

133. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

134. Defendant's duty to use reasonable security measures under 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).

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

136. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

137. Defendant's duty to use reasonable care in protecting confidential data arose not

only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

138. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their computer networks and systems;
- c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;
- d. Failing to adequately train its employees to recognize and contain cyberattacks;
- e. Allowing unauthorized access to Class Members' Private Information;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- g. Failing to timely notify Class Members about the cyberattack regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to have mitigation and back-up plans in place in the event of a cyberattack and data breach.

139. It was foreseeable that Defendant's failure to use reasonable measures to protect

Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

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

141. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyberattack and Data Breach.

142. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit and identity monitoring to all Class Members.

COUNT II

BREACH OF IMPLIED CONTRACT (On Behalf of Plaintiffs and the Class)

143. Plaintiffs re-allege and incorporate by reference paragraphs 1-126 as if fully set forth herein.

144. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts, a component of which required Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

145. Defendant required employee Class Members to provide their personal information, including names, addresses, Social Security numbers, dates of birth, email, and phone number; financial information such as bank account numbers; medical information, and other

personal information, as a condition of their employment. As a condition of Plaintiffs' and Class Members' employment with Defendant, they employee-Class Members provided their personal, financial, and medical information. In so doing, employee-Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify employee-Class Members if their data had been breached and compromised, or stolen.

146. Likewise, through their course of conduct, Defendant and patient-Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of patient Class Members' Private Information. Specifically, patient-Class Members entered into a valid and enforceable implied contract with Defendant when they paid for and received in-home healthcare services from Defendant. The valid and enforceable implied contracts to provide in-home health care services that patient-Class Members entered into with Defendant include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

147. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

148. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

149. Defendant materially breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect Private Information and by failing to provide timely and accurate notice to them that Private Information was compromised as a result of the

data breach.

150. The cyberattack and Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

151. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have provided their confidential Private Information to Defendant.

152. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiffs and the Class)

153. Plaintiffs re-allege and incorporate by reference paragraphs 1-126 as if fully set forth herein.

154. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- (a) Defendant misrepresented material facts to Plaintiffs and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;
- (b) Defendant misrepresented material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;
- (c) Defendant omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Class Members' Private Information;
- (d) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);
- (e) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

155. Defendant knew or should have known that the Preferred Home network and data security practices were inadequate to safeguard the Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

156. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

157. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Preferred Home's network and aggregation of Private Information.

158. The representations upon which current and former employees (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and current and former employees (including Plaintiffs and Class Members) relied on those representations to their detriment.

159. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

160. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

161. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

162. Plaintiffs re-allege and incorporate by reference paragraphs 1-126 as if fully set forth herein.

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

164. Defendants owed a duty to their current and former employees and patients, including Plaintiffs and the Class, to keep their Private Information contained as a part thereof, confidential.

165. Defendant failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiffs and the Class.

166. Defendant allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiffs and the Class, by way of Defendant's failure to protect the Private Information.

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

168. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to Defendant as part of their special relationship with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

169. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's 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.

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

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

172. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

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

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

174. Plaintiffs re-allege and incorporate by reference paragraphs 1-126 as if fully set forth herein.

175. At all times during Plaintiffs' and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class's Private Information that Plaintiffs and the Class provided to Defendant.

176. As alleged herein and above, Defendant's relationship with Plaintiffs and the Class was governed by terms and expectations that Plaintiff's and the Class's Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

177. Plaintiffs and the Class provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

178. Plaintiffs and the Class also provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

179. Defendant voluntarily received in confidence Plaintiffs' and the Class's Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

180. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Class's Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

181. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and the Class have suffered damages.

182. But for Defendants' disclosure of Plaintiffs' and the Class's Private Information in violation of the parties' understanding of confidence, their Private Information would not have

been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class's Private Information as well as the resulting damages.

183. The injury and harm Plaintiffs and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class's Private Information. Defendant knew or should have known their methods of accepting and securing Plaintiffs' and the Class's Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class's Private Information.

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

Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

185. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and behalf of all others similarly situated, respectfully request that this Court:

- A. Certifying this case as a class action pursuant to New York's C.P.L.R. § 901(a), appointing Plaintiffs as Class Representatives, and the undersigned as Class Counsel;
- B. Award monetary, punitive and actual damages and/or restitution, as appropriate;
- C. Award declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining Preferred Home from continuing the unlawful practices as set forth above;
- D. Grant prejudgment interest to the extent allowed by the law;
- E. Award all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and
- F. Enter such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

DATED: May 14, 2021

Respectfully submitted,

/s/ Roopal P. Luhana
Roopal P. Luhana, Esq.
Steven Cohn, Esq.
CHAFFIN LUHANA, LLP
600 Third Avenue, 12th Floor
New York, NY 10016
Phone: 888-480-1136
Fax: 888-499-1123
luhana@chaffinluhana.com
cohn@chaffinluhana.com


Gary E. Mason
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

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


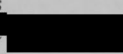
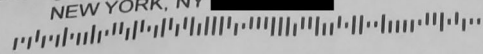
**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

 **Preferred**
HOME CARE OF NEW YORK
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 10, 2021

G3050-L04-0015765 T00041 P002 *****AUTO**5-DIGIT 10026
 LISA SIMMONS
NEW YORK, NY 



Dear Lisa Simmons:

Assistcare Home Health Services LLC dba Preferred Home Care of New York/Preferred Gold (“we”) has always been and continues to be committed to the privacy and confidentiality of its caregivers. We are writing to notify you about a recent data security incident we experienced which may have involved your personal information. We recognize the concern this may cause, and we write to inform you of the steps we have taken to resolve the incident.

On January 9, 2021 we identified a disruption within our network and learned that an unauthorized third party had accessed our computer network. Upon identifying the issue, we promptly initiated an internal investigation, and hired a leading computer forensics firm to examine our network and to confirm the security of our computer systems. Through the investigation, we confirmed the unauthorized third party no longer has access to our network, but confirmed that they were able to access and acquire certain files on our network for the time period between January 8th and 10th, 2021.

We believe that the likelihood of any one particular individual's information being impacted is very low, but we cannot rule out that possibility. Currently, we are not aware of any fraudulent activity or misuse of anyone's information as a result of the incident. Furthermore, we do not believe that the use of personal information was the primary motive behind the third party's actions. Nonetheless, because your information was saved to computer systems that the unauthorized party was able to access, we are writing to alert you of the incident and encourage you to monitor your personal accounts. The type of information accessed varied depending on the individual, but may have included your name, contact and demographic information such as address, email, phone number, and date of birth; financial information such as bank account number; and Social Security number; and medical information related to health assessments, physicals, drug screens, vaccinations and TB tests, as well as FMLA and worker's compensation claims.

EXHIBIT B

 Preferred
HOME CARE OF NEW YORK
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

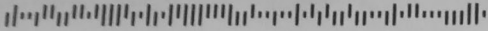
March 10, 2021



G3050-L02-0047583 T00151 P003 *****AUTO**5-DIGIT 11212

KELLY SMALL

BROOKLYN, NY



Dear Kelly Small:

Assistcare Home Health Services LLC dba Preferred Home Care of New York/Preferred Gold ("we") has always been and continues to be committed to the privacy and confidentiality of its current and former employees. We are writing to notify you about a recent data security incident we experienced which may have involved your personal information. We recognize the concern this may cause, and we write to inform you of the steps we have taken to resolve the incident.

On January 9, 2021 we identified a disruption within our network and learned that an unauthorized third party had accessed our computer network. Upon identifying the issue, we promptly initiated an internal investigation, and hired a leading computer forensics firm to examine our network and to confirm the security of our computer systems. Through the investigation, we confirmed the unauthorized third party no longer has access to our network, but confirmed that they were able to access and acquire certain files on our network for the time period between January 8th and 10th, 2021.

We believe that the likelihood of any one particular individual's information being impacted is very low, but we cannot rule out that possibility. Currently, we are not aware of any fraudulent activity or misuse of anyone's information as a result of the incident. Furthermore, we do not believe that the use of personal information was the primary motive behind the third party's actions. Nonetheless, because your information was saved to computer systems that the unauthorized party was able to access, we are writing to alert you of the incident and encourage you to monitor your personal accounts. The type of information accessed varied depending on the individual, but may have included your name, contact and demographic information such as address, email, phone number, and date of birth; financial information such as bank account number; and Social Security number. For some individuals it also included medical information related to FMLA or worker's compensation claims.

Out of an abundance of caution, we are also offering you a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**