UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

LAURIE GAY GERBER, on behalf of herself and all others similarly situated,

Plaintiff,

v.

NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC.,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Laurie Gay Gerber ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint against the above-captioned Defendants, Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJ&A") (collectively, the "Defendants"), upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. Northwell is the largest health system in the state of New York.

2. In the course of serving patients in New York and the surrounding area, Northwell collects a significant amount of data, including protected health information ("PHI") under the Health Insurance Portability and Accountability Act ("HIPAA"), consisting of each patients' name, date of birth, address, medical record number, hospital account number, and clinical information[1] (collectively, the "Personal Identifiable Information" or "PII"). This is an extremely sensitive set of information which necessitates the utmost care in terms of protection from cybercriminals.

3. When patients and employees disclosed this PII to Northwell, they did so under the impression that this PII would be protected in a manner consistent with how sensitive and valuable this subset of PII is.

4. However, on November 3, 2023, it was disclosed that the PII of nearly four million current or former Northwell patients, including the PII of Plaintiff and the Class, had been

[1] Clinical information is defined by PJ&A as "the name of the treatment facility, the name of health care providers, admission diagnosis, date(s) and time(s) of service, files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries or progress notes … diagnosis, laboratory and testing results, medical history including family history, surgical history, social history, medications, allergies, and/or other observational information."

compromised in connection with a cyberattack that was discovered on May 2, 2023 (the "Data Breach"). According to the Notice of Data Breach (the "Notice") received from PJ&A by Plaintiff Gerber, the Data Breach occurred when Northwell's third-party medical technology services vendor for transcription and dictations services – Perry Johnson & Associates, Inc. – had its computer systems compromised. PJ&A was in possession of Plaintiff's and the Class' PII because, according to the Notice, "[i]n order to perform … services, PJ&A receives personal health information regarding Northwell patients."

5. The conduct of PJ&A with respect to the Data Breach is egregious: (1) PJ&A's systems were first compromised on March 27, 2023 but PJ&A was completely unaware of the breach until over six weeks later (on May 2, 2023); (2) PJ&A became cognizant of the Data Breach on May 2, 2023 but failed to notify Northwell until July 21, 2023; (3) PJ&A failed to state in its Notice how the Data Breach specifically occurred, the remedial measures, if any,taken to protect the PII still in its possession, and how PJ&A intends to prevent this from happening again. Northwell's conduct is similarly disturbing: (1) as the very entity responsible for hiring PJ&A, Northwell is offering no remediation whatsoever and (2) Northwell still has not disseminated a notice to its patients. This means that many patients found out that they were victims of the Data Breach from PJ&A, an entity they might never have ever heard of. Resultingly, many members of the Class might have no idea that their sensitive information was compromised because they might have disposed of PJ&A's Notice.

6. As such, Plaintiff, on behalf of herself and all others similarly situated, brings this action, seeking actual damages, punitive damages, restitution, statutory damages, injunctive relief, and a declaratory judgment, as well as any other relief this Court deems just and proper, for Defendants' negligence, and, in the alternative to breach of contract, unjust enrichment.

II. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interests and costs, there are well over 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than at least one Defendant (namely, Plaintiff Gerber is a New York resident and Defendant PJ&A is domiciled in Nevada).

8. This Court has personal jurisdiction over Defendant Northwell because Northwell maintains its principal place of business in New Hyde Park, New York. Furthermore, Defendant Northwell intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing medical services in New York. Additionally, this Court has personal jurisdiction over Defendant PJ&A because PJ&A intentionally availed itself of this jurisdiction by choosing to do business in New York.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Northwell is located in this District, both Defendants conduct business in this District and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in this District. Additionally, Plaintiff is located in this District.

III. PARTIES

Plaintiff Laurie Gay Gerber

10. Plaintiff Gerber is a resident and citizen of the State of New York, residing in Suffolk County. Plaintiff was a patient at Northwell and, therefore, provided Northwell with her name, address, date of birth and PHI (as defined *Supra*, at 1). Plaintiff received the Notice, dated

November 3, 2023. By way of the Notice, Plaintiff was informed that her sensitive PII was compromised in the Data Breach.

Defendant Northwell

11. Defendant Northwell Health, Inc. is a New York not-for-profit corporation with its principal place of business located at 2000 Marcus Avenue, New Hyde Park, New York 11042.

Defendant PJ&A

12. Defendant Perry Johnson & Associates, Inc. is a Nevada corporation with its principal place of business located at 1489 W. Warm Springs Road, Henderson, Nevada 89014.

IV. FACTUAL ALLEGATIONS

Defendants' Businesses

13. Northwell is a major hospital system located in New York, providing care to citizens of New York as well as the surrounding states. Northwell has over 900 different locations where it provides service, with many of those locations clustered in or around Long Island, New York and New York City, New York.

14. PJA is a Nevada based corporation that, according to its website, "provides medical transcription services to various healthcare organizations."

15. Northwell hired PJ&A, a medical technology company, for the transcription and dictation of Northwell's patient data. Northwell has used PJ&A's services for a variety of purposes, including the storage of Plaintiff's and Class members' PII. Like millions of New Yorkers, Plaintiff's and the Class members' PII was given to Northwell for health purposes and was entrusted to Northwell. In undertaking this responsibility, Northwell was obligated to only hire vendors who maintain adequate data security practices.

16. In the ordinary course of working for or receiving health care services from Northwell, patients are required to provide, at a minimum, their PII. This PII is then paired with PHI attributable to a given patient, and the PHI then becomes identifiable as a result.

17. Prior to receiving care and treatment from Northwell, Plaintiff Gerber was required to and did in fact turn over much of the private and confidential information listed in this Complaint.

18. Additionally, with respect to PHI, Northwell may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

19. Northwell also creates and maintains a considerable amount of PHI in the course of providing medical care and treatment. This PHI includes, but is not limited to, billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from Northwell. All of this information is then provided to PJ&A for the purposes of transcription or dictation.

20. According to Northwell's website, "patients are our number one priority and we believe that patient privacy is an integral part of the health care we provide you." The website continues, "[t]o ensure the development of a lasting bond of trust with our patients, we have many safeguards to protect the privacy and security of your personal information… We also have many policies in place to protect the privacy and security of your personal information and our employees are educated from the moment they are hired and continually after, to respect and protect patient privacy."

21. According to Northwell's Notice of Privacy Practices (which can also be found on the Northwell website), "[we are] required by law to make sure that the information that identifies you is kept private." And while the Notice of Privacy Practices discusses each of the various uses and disclosures of patient health information, it emphasizes that such uses and disclosures are only done so with written authorization. Thus, Northwell (and therefore, the third parties it hires, such as PJ&A) promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

22. Due to the highly sensitive and personal nature of the information Northwell acquires, Northwell recognizes patients' right to privacy on its website, and it promises in its Notice of Privacy Practices, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in the Data Breach.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' PII, Defendants assumed legal and equitable duties and knew that they were responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

24. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII.

25. Plaintiff and the Class members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

The Data Breach

26. On or about October 31, 2023, PJ&A began notifying victims as well as states' attorneys general of the Data Breach. This was done in part by disseminating a "Notice of Data Security Incident" letter to victims of the Data Breach. That Notice, which was posted online, states in relevant part:

> PJ&A, which provides medical transcription services to various healthcare organizations, is committed to protecting the privacy and security of the information we maintain. On October 31, 2023, we began mailing notification letters to certain individuals whose information may have been involved in a data security incident that PJ&A experienced.
>
> An unauthorized party gained access to the PJ&A network between March 27, 2023, and May 2, 2023, and, during that time, acquired copies of certain files from PJ&A systems. We retained a cybersecurity vendor to assist with the investigation, contain the threat, and further secure our systems. We also directed its vendor to review the affected files and determine their precise contents. Importantly, this incident did not involve access to any systems or networks of PJ&A's healthcare customers.
>
> PJ&A determined that the involved files contained personal health information belonging to certain individuals. The information varies per individual but may include some or all of the following: name, date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service. The information accessed by the unauthorized party did not contain credit card information, bank account information or usernames or passwords. For some individuals, however, the impacted data may have also included Social Security numbers, insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility, and the name of healthcare providers. Beginning on or about September 29, 2023, PJ&A provided the results of its review to its affected customers and began working with them to notify individuals whose information was identified during the review.
>
> While we have no evidence that individuals' information has been misused for the purpose of committing fraud or identity theft, individuals whose information may have been involved are encouraged to review the notification they receive, including guidance on what they can do to protect themselves, should they feel it is appropriate to do so.
>
> We value individuals' privacy and deeply regret any concern that this incident might cause. To help prevent something like this from happening again, PJ&A

continues to review its safeguards and has implemented additional technical security measures to further protect and monitor its systems.

A dedicated toll-free call center has been established to support affected individuals with questions about the incident. The call center can be reached at (833) 200-3558, Monday to Friday, between 8:00 a.m. and 11:59 p.m. Eastern Time, excluding major U.S. holidays.

This notice is being provided by PJ&A, incorporated as Perry Johnson & Associates, Inc., in its capacity as a business associate to multiple covered entities, and in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. PJ&A has notified impacted individuals and relevant regulatory bodies, including the U.S. Department of Health and Human Services (HHS).

27. Victims received a similar Notice by mail, which stated in relevant part:

Perry Johnson & Associates … is providing this letter to inform you of an event that may affect your personal health information. This letter provides details of the event, our response, and the resources available to you to help protect your personal health information from possible misuse[.]

Who is PJ&A and Why Did We Have Your Information? PJ&A serves as a vendor to Northwell Health, Inc. and its subsidiaries and affiliates…. PJ&A provides transcription and dictation services to Northwell. In order to perform these services, PJ&A receives personal health information regarding Northwell patients.

What Happened? PJ&A became aware of a data security incident impacting our systems on May 2, 2023… Through our investigation, we determined that the unauthorized access to our systems occurred between March 27, 2023 and May 2, 2023, and that the unauthorized access to Northwell patient data specifically occurred between April 7, 2023 and April 19, 2023.

On July 21, 2023, PJ&A notified Northwell that an unauthorized party had accessed and downloaded certain files from our systems. PJ&A had preliminarily determined that Northwell data was impacted on May 22, 2023 and, by September 28, 2023, confirmed the scope of the Northwell data impacted.

28. There were multiple critical failures on the part of PJ&A: (1) PJ&A's systems were first compromised on March 27, 2023 but was completely unaware of the breach until over six weeks later (on May 2, 2023); (2) PJ&A became cognizant of the Data Breach on May 2, 2023,

but failed to notify Northwell until July 21, 2023; and (3) PJ&A failed to state in its Notice how the Data Breach specifically occurred, the remedial measures, if any, taken to protect the PII still in its possession, and how PJ&A intends to prevent this from happening again.

29. There were also multiple failures on the part of Northwell: (1) as the entity responsible for hiring PJ&A, Northwell is offering no remediation whatsoever and (2) Northwell never disseminated a notice to its patients. This means that many patients found out that they were victims of the Data Breach from PJ&A, an entity they might never have heard of. Indeed, PJ&A even introduces itself in a section called "Who is PJ&A and Why Did We Have Your Information" in the Notice.

30. PJ&A's omissions within the Notice are also notable: PJ&A failed to illuminate how the unauthorized actors initially gained access, why PJ&A failed to detect the intrusion(s) of these unauthorized actors, and how PJ&A intends to ensure that these types of incidents do not happen again. These critical points remain unclear.

31. But what is clear from the Notice is that cybercriminals did, in fact, access and view Plaintiff's and Class members' PII and PHI during the period in which the cybercriminals had unfettered access to PJ&A's IT network, as that is the *modus operandi* of cybercriminals who commit such attacks.

32. PJ&A did not implement or maintain adequate measures to protect its current and former employees' and patients' PII and PHI. Further, Northwell failed to oversee and maintain PJ&A's use, storage, collection, and protection of the PII and PHI at-issue.

33. On information and belief, the PII and PHI compromised in the files accessed by hackers was not encrypted. This can be presumed given the hackers were able to access the data that is listed as compromised in the Notice.

34. Moreover, the removal of PHI and other PII from PJ&A's system demonstrates that this cyberattack was targeted due to its status as a healthcare technology provider that houses sensitive PII and PHI from entities like Northwell.

35. Due to PJ&A's incompetent security measures and its incompetent response to the Data Breach, Plaintiff and the Class members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever. Equally troubling, Plaintiff and the Class members now face a present and substantial risk of disclosure of their sensitive and deeply private medical information which will impact them in perpetuity.

36. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII and PHI, PJ&A and Northwell provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling patients' PII and PHI, inadequate oversight of third-party vendors, and inadequate employee training regarding how to access, handle and safeguard this information.

37. Defendants failed to adequately adopt and train its employees on even the most basic of information security protocols, including: storing, locking, encrypting and limiting access to current and former employees and patients' highly sensitive PHI; implementing guidelines for accessing, maintaining and communicating sensitive PHI; and protecting sensitive PHI by implementing protocols on how to utilize such information.

38. Defendants' collective failures caused the unpermitted disclosure of Plaintiff's and Class members' PII to an unauthorized third party and put Plaintiff and the Class members at serious, immediate, and continuous risk of identity theft and fraud.

39. The Data Breach that exposed Plaintiff's and Class members' PHI was caused by Defendants' violation of their obligations to abide by best practices and industry standards concerning information security practices and processes.

40. Defendants failed to comply with security standards or to implement security measures that could have prevented or mitigated the Data Breach.

41. Defendants failed to ensure that all personnel with access to patients' PII and PHI were properly trained in retrieving, handling, using and distributing sensitive information.

The Breach Was Foreseeable

42. Defendants both had weighty obligations created by HIPAA, industry standards, common law and the promises and representations made to Plaintiff and Class members to keep their PII and PHI confidential and to protect the information from unauthorized access and disclosure.

43. Plaintiff and Class members provided their PII and PHI to Northwell with the reasonable expectation and mutual understanding that Northwell and any third parties that it works with would comply with their obligations to keep such information confidential and secure from unauthorized access.

44. Defendants' data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the Data Breach.

45. Data breaches, including those perpetrated against the healthcare sector of the economy, have become extremely widespread.

46. For example, in 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[2] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[3]

47. Defendants were aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

48. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, 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), BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

49. In 2021 alone there were over 220 data breach incidents.

50. These approximately 220 data breach incidents impacted nearly 15 million individuals.

51. Indeed, cyberattacks have become so prevalent that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller

---

[2] IDENTITY THEFT RESOURCE CENTER, *2019 End-of-Year Data Breach Report*, (Jan. 8, 2020), https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

[3] *Id.*

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."[4]

52. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[5]

53. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful and nefarious ways. PII and PHI can be used to distinguish, identify or trace an individual's identity, such as their name and medical records. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

54. Given the nature of the Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of nefarious ways.

55. Cybercriminals who possess the Class members' PII and PHI can readily obtain Class members' tax returns or open fraudulent credit card accounts in the Class members' names.

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

---

[4] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[5] HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited November 14, 2023).

Defendants Failed to Follow FTC Guidelines

57. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

58. According to the FTC, the need for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

60. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[6]

61. 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.[7]

62. 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

---

[6] FEDERAL TRADE COMMISSION, *Protecting Personal Information, A Guide for Business*, (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[7] *Id.*

on the network; and verify that third-party service providers have implemented reasonable security measures.[8]

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

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

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

66. Defendants were at all times fully aware of their obligations to protect the PII and PHI of its patients and employees. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Failed to Meet Industry Standards

67. As detailed above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

68. Several best practices have been identified that, at a minimum, should be implemented by healthcare providers such as Northwell, including but not limited to: educating all employees; utilizing strong passwords; implementing multi-layer security, including firewalls,

[8] *Id.*

anti-virus, and anti-malware software; encryption, making data unreadable without a key; employing multi-factor authentication; backing up data; limiting which employees can access sensitive data.

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

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

71. These foregoing frameworks are existing and applicable industry standards in the healthcare industry. Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendants Failed to Comply with HIPAA

72. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information. Defendants are HIPAA covered entities, and thus have extensive obligations to protect patient health information.

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

74. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI and PII like the data Defendants left unguarded.

75. 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).

76. A data breach such as the one Defendants experienced, is 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

77. Data breaches are Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *See* definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).

78. Defendants' Data Breach resulted from a combination of insufficiencies which demonstrate that Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants' Breach

79. Defendants breached their express and implied obligations to Plaintiff and the Class members and were otherwise negligent and/or reckless because they failed to properly maintain and safeguard its computer systems, network and data.

80. Defendants' 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 cyber-attacks;

b. Failing to adequately protect consumers' PHI and other PII;

c. Failing to properly monitor their own data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to properly monitor third party vendors;

e. Failing to apply all available and necessary security updates;

f. Failing to install the latest software patches, update firewalls, check user account privileges, or ensure proper security practices;

g. Failing to practice the principle of least-privilege and maintain credential hygiene;

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

j. Failing to properly train and supervise employees in the proper handling of inbound emails;

k. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

l. 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);

m. 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);

n. 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);

o. 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);

p. 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);

q. Failing to ensure compliance with HIPAA security standard rules by itheir workforces in violation of 45 C.F.R. § 164.306(a)(4);

r. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

s. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they 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 (definition of encryption).

81. As a result of allowing their computer systems to fall into dire need of security upgrading and their inadequate procedures for handling cybersecurity threats, Defendants negligently and unlawfully failed to safeguard Plaintiff's and the Class members' PII and PHI.

82. Accordingly, as detailed below, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal medical information.

Data Breaches Are Disruptive and Harm Consumers

83. Hacking incidents and data breaches at medical facilities and companies such as Defendants are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

84. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.

85. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.

86. 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."[9]

87. 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.

88. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or 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 regarding a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

89. 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.

90. The FTC recommends that identity theft victims take various steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to 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.

[9] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

91. Theft of PII and PHI is gravely serious. PII and PHI is an extremely valuable property right.

92. 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 a doubt that PII and PHI has considerable market value.

93. Theft of PHI, in particular, is momentous: "[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, insurance and payment records, and credit report may be affected."

94. 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.

95. 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 PII, PHI, and/or financial information is stolen and when it is used.

96. 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.[10]

[10] *Id.* at 29.

97. PII and PHI 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.

98. There is a strong probability that entire batches of information stolen in the Data Breach have been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

99. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

100. Sensitive PII and PHI can sell for as much as $363 per record according to the Infosec Institute.[11]

101. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

102. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

103. Medical information is especially valuable to identity thieves.

104. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

105. For this reason, Defendants knew or should have known about these dangers and strengthened their network and data security systems accordingly. Defendants were put on notice

[11] Ashiq JA, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC INSTITUTE, (July 27, 2015), https://resources.infosecinstitute.com/topics/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/.

of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Harm to Plaintiff

106. On or about November 3, 2023, Plaintiff received notice from Defendant PJ&A that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's PII and PHI was compromised as a result of the Data Breach.

107. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

108. Plaintiff suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendants obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

109. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

110. This Action is properly maintainable as a Class Action.

111. Plaintiff brings this nationwide class on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure. The "Nationwide Class" that the Plaintiff seeks to represent is defined as follows:

> **Class Definition.** All individuals residing in the United States whose PII and/or PHI was compromised on the Data Breach announced by PJ&A in October and November of 2023.

112. Excluded from the Class are: Defendants and Defendants' subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

113. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

114. **Numerosity**. Northwell reports that the Data Breach compromised PII and PHI of nearly four million current and former patients. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

115. **Commonality**. 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 Defendants unlawfully used, maintained, lost or disclosed Plaintiff's and Class members' PII and PHI;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class members to safeguard their PII and PHI;

f. Whether Defendants breached its duty to Class members to safeguard their PII and PHI;

g. Whether computer hackers obtained Class members' PII and PHI in the Data Breach;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and

k. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

116. **Typicality**. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII and PHI, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendants' uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

117. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class members in that she has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel

experienced in complex consumer class action litigation, including data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

118. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class' common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

119. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

120. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

121. **Predominance**. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

122. This proposed class action does not present any unique management difficulties.

COUNT I

NEGLIGENCE

123. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

124. Northwell knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the PII from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

125. The duty included obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Northwell's duties included the responsibility to design, implement, and monitor its and its third-party vendors' data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

126. Northwell and PJ&A owed a duty of care to Plaintiff 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 PII.

127. Northwell and PJ&A owed a duty of care to safeguard the PII due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the PII.

128. Northwell's and PJ&A's duty of care to use (and to ensure that their respective third-party vendors used) reasonable security measures arose as a result of the special relationship that existed between Northwell and PJ&A and those individuals who entrusted them with their PII, which is recognized by laws and regulations including but not limited the FTC Act, HIPAA, as well as common law. Northwell and PJ&A were in a position to ensure that their own (and their vendor's) systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

129. In addition, Northwell and PJ&A 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.

130. Similar duties arise under Northwell's collection of PHI pursuant to HIPAA.

131. Additionally, Northwell's and PJ&A's duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because they are bound by industry standards to protect PII that they either acquire, maintain, or store.

132. Defendants breached their duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class members' PII, as alleged and discussed above.

133. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiff and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance, data transfer and storage industries.

134. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

135. The imposition of a duty of care on Defendants to safeguard the PII it maintained, transferred, stored or otherwise used is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiff and Class members as a result of the Data Breach.

136. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members are at a current and ongoing imminent risk of identity theft, and Plaintiff and Class members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of

pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their PII; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to PII, which remains in Northwell's and PJ&A's respective control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

137. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

138. Northwell's and PJ&A's negligent conduct is ongoing, in that they (and their third-party vendors) still hold the PII of Plaintiff and Class members in an unsafe and unsecure manner.

139. Plaintiff and Class members are also entitled to injunctive relief requiring the Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT II

BREACH OF EXPRESS AND IMPLIED CONTRACT

140. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

141. Northwell entered into contracts with customers, agents, and businesses to provide healthcare and health insurance services. These services included data security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to Northwell.

142. Plaintiff and Class members were parties to such contracts, as it was their PII that Northwell agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class members was the direct and primary objective of the contracting parties.

143. Northwell knew that if it were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

144. Northwell breached its contracts with customers by, among other things, failing to adequately secure Plaintiff's and Class members' PII, and, as a result, Plaintiff and Class members were harmed by Northwell's failure to secure their PII.

145. As a direct and proximate result of Northwell's breach, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their PII, which remains in either Defendant's control, and which is subject to further breaches, so long as each Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

146. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT III

UNJUST ENRICHMENT

147. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

148. This Count is in the alternative to Breach of Express and Implied Contract, Count II.

149. Plaintiff and the Class members conferred a benefit on Defendants with their money and/or valuable data. Specifically, they purchased medical services from Northwell and in so doing also provided both Defendants with their PII and PHI. In exchange, Plaintiff and the Class members should have received from Northwell the medical goods and services that were the subject of the transaction and should have had their PII and PHI protected with adequate data security.

150. Defendants knew that Plaintiff and the Class members conferred a benefit which Defendants accepted. Defendants both profited from these transactions and used the PII and PHI of Plaintiff and Class members for business purposes.

151. In particular, the Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and the Class members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and the Class members, on the other hand, suffered as a direct and proximate result of Defendants' decisions to prioritize their own profits over necessary and requisite security.

152. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and the Class members, because Defendants

failed to implement appropriate data management and security measures that are mandated by industry standards.

153. Defendants failed to secure Plaintiff's and the Class members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

154. Defendants acquired the PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

155. Had Plaintiff and the Class members known that Defendants had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Northwell.

156. Plaintiff and the Class members have no adequate remedy at law.

157. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII and PHI is used; (c) the compromise, publication, and/or theft of their PII and PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (e) lost opportunity costs associated with efforts 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 identity theft; (f) the continued risk to their PII and PHI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII and PHI in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class members.

158. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class members have suffered and will continue to suffer other forms of injury and/or harm.

159. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and the Class Members overpaid for Northwell's services.

PRAYER FOR RELIEF

160. WHEREFORE, Plaintiff, on her own behalf and on behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For an award of actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of punitive damages, as allowable by law;

D. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendants' possession;

E. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

161. Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: November 14, 2023

Respectfully Submitted,

/s/ *Israel David*

Israel David
Blake Hunter Yagman
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, New York 10004
Tel.: 212-739-0622
Fax: 212-739-0628
Email: *israel.david@davidllc.com*
blake.yagman@davidllc.com

Attorneys for Plaintiff Gerber and the Proposed Class