UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CARLA TRACY, DARRYL BOWSKY, and DEBORAH HARRINGTON, individually and on behalf of all others similarly situated, **Plaintiffs,** **v.** **ELEKTA, INC., and NORTHWESTERN MEMORIAL HEALTHCARE**	**Case No. 1:21-cv-02851** **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Carla Tracy, Darryl Bowsky, and Deborah Harrington ("Plaintiffs"), bring this Consolidated Amended Class Action Complaint, on behalf of themselves and all others similarly situated (the "Nationwide Class" and the "Illinois Subclass"), against Defendants Elekta, Inc. ("Elekta" or "Defendant Elekta") and Northwestern Memorial Healthcare ("Northwestern" or "Defendant Northwestern") (collectively "Defendants") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

NATURE OF CASE

1. Elekta specifically markets and holds itself out as being committed to Cybersecurity stating: "In today's interconnected digital healthcare ecosystem, the

highest cybersecurity standards are critical for patient safety and data protection."[1] Elekta further markets itself as being "committed to advancing cybersecurity in medical devices and maintaining the protection of patient, personal and business data."[2]

2. This Class Action arises from Defendants' individual and collective failures to secure and protect Plaintiff's' and Class Members' personal information from unauthorized disclosure, exfiltration, and theft by criminal third parties. There are three types of highly personal information at issue in the case: (1) personal identifying information ("PII"), including names, Social Security Numbers, dates of births, and addresses; (2) protected health information ("PHI"), including clinical information related to cancer treatment, medical record numbers, medical histories, dates of service, treatment plans, physician names, diagnosis, prescription information, and health insurance information; and (3) and protected genetic information ("PGI").

3. PII, PHI and PGI are collectively referred to herein as "Sensitive Information."

4. Cancer is a genetic disease - that is, cancer is caused by certain changes to genes that control the way human cells function, especially how they grow and

[1] https://www.elekta.com/software-solutions/product-security (last visited Jan. 22, 2022).
[2] *Id*.

divide. Certain gene changes, or mutations, can cause cells to evade normal growth controls and become cancer. For example, some cancer-causing genes change or increase the production of a protein that makes cells grow.[3] Genetic tests for hereditary cancer can help determine whether certain patients are more susceptible to developing certain types of cancer and whether patients will respond to certain types of medications. And, therefore, genetic testing and evaluation, including DNA analysis and sequencing, is common in the diagnosis and treatment plans for cancer patients.[4] Biomarker tests, for example, which may be referred to as a companion diagnostic test, is paired with specific treatment plans to help select the best course of treatment.[5] Biomarker testing is routinely conducted to select treatment for people who are diagnosed with certain types of cancer -including non-small cell lung cancer, breast cancer and colorectal cancer.[6] These genetic test results and PGI are typically included in a person's medical records that relate to medical diagnosis and treatment.

5. As part of the ongoing development of science and medicine, and during the treatment course, "oncology clinics around the world generate enormous amounts

---

[3] https://www.cancer.gov/about-cancer/causes-prevention/genetics (last visited Jan. 22, 2022).
[4] https://www.cancer.gov/about-cancer/causes-prevention/genetics/genetic-testing-fact-sheet#:~:text=A%20different%20type%20of%20genetic,be%20used%20to%20guide%20treatment. (last visited Jan. 22, 2022).
[5] https://www.cancer.gov/about-cancer/treatment/types/biomarker-testing-cancer-treatment (last visited Jan. 22, 2022).
[6] *Id*.

of data."[7] In an effort to support and streamline the data from multiple sources to improve patient care and research, Elekta maintains a first-generation cloud-based data storage system that serves cancer healthcare providers worldwide.[8] The cloud-based system is integrated with Elekta software to help medical professionals with patient management by providing a "complete picture" of the patient and their care pathways.[9]

6. Elekta promotes its products as a "single source of truth"[10] and offers a "suite of cloud based clinical and business intelligence applications" that (1) collect, aggregate, and analyze information from multiple data systems; (2) use real time dashboards for effective analysis to improve practice; and (3) ensure compliance and support research with standardized data collection and reporting.[11]

7. Elekta's registry systems and analysis tools help its customers, like Defendant Northwestern, ensure "policy compliance and provide a rich pool of data for benchmarking and clinical research."[12]

---

[7] https://www.elekta.com/software-solutions/knowledge-management/registries/data-alliances (last visited Jan. 20, 2022).
[8] https://www.elekta.com/software-solutions/cloud-solutions/ (last visited Jan. 23, 2022).
[9] https://www.elekta.com/software-solutions/ (last visited Jan. 23, 2022).
[10] https://www.elekta.com/software-solutions/#care-management (last visited Jan. 23, 2022).
[11] https://www.elekta.com/software-solutions/#knowledge-management (last visited Jan.20, 2022).
[12] *Id.*

8. Defendant Northwestern utilized Elekta's system to help facilitate legally required cancer reporting to state agencies. As part of the reporting requirements, Northwestern was required to provide Illinois with detailed medical information and all "medical, pathological, and other pertinent records and logs related to cancer diagnosis and treatment".[13]

9. The Elekta database containing the Sensitive Information that Northwestern utilized to comply with Illinois cancer reporting requirements was hacked, accessed, exfiltrated, and stolen by a third-party cybercriminal.[14]

10. The Data Breach, however, was not limited to Northwestern's patient data. Between April 2, 2021 and April 20, 2021, Elekta experienced a ransomware attack and subsequent data breach that allowed hackers to gain unauthorized access to Elekta's cloud-based database ("Data Breach") that allowed access to and exfiltration of the personal and medical information of Elekta's oncology patients throughout the United States.

11. Due to Elekta's inadequate data security, which failed to comply with federal and state laws, and further failed to meet industry data privacy standards, an unauthorized third party used compromised credentials to gain access to Elekta's

[13] https://www.ilga.gov/commission/jcar/admincode/077/077008400B01100R.html (last visited Jan. 22, 2022).
[14] Defendants often refer to cybercriminals or cyberattackers as merely "threat actors".

digital environment. Thereafter, the unauthorized third-party gained access to, and exfiltrated the files and records of various businesses customers of Elekta, including Northwestern Memorial HealthCare, Renown Health, St. Charles Health System, Carle Health, Cancer Centers of Southwest Oklahoma, LLC, Lifespan, Southcoast Health, and Yale New Haven Health.

12. In response, on or about April 28, 2021, Elekta engaged in a forensic investigation and thereafter announced that "Elekta must conclude that all data within Elekta's first-generation cloud system was compromised."[15] Upon information and belief, the files and records that were accessed, compromised, exfiltrated and stolen included the Sensitive Information of Plaintiffs and the Class Members.

13. Furthermore, as a result of the Data Breach, Elekta temporarily was forced to take its system offline until the security vulnerabilities could be identified and addressed, which in turn prevented or delayed treatment for many cancer patients across the United States.

14. Healthcare providers and their vendors, including Defendant Elekta, that collect and store patient Sensitive Information have statutory, regulatory, and common law duties to safeguard that information and ensure that it remains private and protected against foreseeable criminal activity.

[15] https://www.saintpetershcs.com/News/2021/Saint-Peter%E2%80%99s-University-Hospital-Notified-of-Data (last visited Jan 22, 2022).

15. Defendants breached their statutory, regulatory, common law and contractual duties as discussed herein.

16. Defendant Northwestern also expressly and impliedly promised Plaintiffs and Class Members that it would maintain the privacy and confidentiality of their Sensitive Information.

17. Defendant Northwestern's patients, including Plaintiffs, entered into implied contracts with Defendant Northwestern as part of the medical services provided and/or involvement in clinical trials whereby Plaintiffs and Class Members reasonably expected that their Sensitive Information that they entrusted to Northwestern, as part of their medical treatment, would remain confidential and would not be shared or disclosed to criminal third parties. The implied promises included an understanding that Defendant Northwestern would take steps to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information. Defendant, individually and by and through its agent Elekta, breached these contractual duties by failing to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information.

18. As a result of Defendants' individual and collective failures to implement and follow reasonable security procedures, Plaintiffs' and Class Members' Sensitive Information was accessed and acquired by criminal networks placing

Plaintiffs and the Class Members at risk for identity theft. Plaintiffs and Class Members have suffered numerous actual, concrete, and imminent injuries as a direct result of the Data Breach, including, but not limited to: (a) the disclosure, compromise and theft of their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with the time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) the emotional distress, stress, nuisance, and annoyance of the responding to and resulting from the Data Breach; (e) the actual and/or imminent injury arising from the actual and/or potential fraud and identity theft posed by their Sensitive Information being placed in the hands of the ill-intentioned hackers and/or criminals; (f) damages to and diminution of value of their Sensitive Information entrusted to Defendants; (g) the actual damages in the difference between the services that should have been delivered and the services that were actually delivered; (h) the continued risk to their Sensitive Information and personal identity, which requires further protection; and (i) statutory damages provided under 410 ILCS 513 (Illinois Genetic Information Privacy Act ("GIPA")).

JURISDICTION AND VENUE

19. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs and at least one member of the putative Class, as defined below, are citizens of a different state than

Defendant Elekta, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

20. This Court has supplemental jurisdiction over all claims involving the Illinois Subclass and Defendant Northwestern as the claims are related to the claims against Defendant Elekta, for which this Court has original jurisdiction, and the Illinois Subclass claims against Northwestern form part of the same case and controversy between the Parties. The presence of Northwestern does not destroy the minimal diversity under 28 U.S.C. § 1332(d)(2).

21. This Court has general personal jurisdiction over Defendant Elekta because Elekta maintains its United States principal place of business at 400 Perimeter Center Terrance, Suite 50, Dunwoody, Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Georgia to many businesses nationwide.

22. Defendant Northwestern has agreed to consent to this Court's specific personal jurisdiction by Stipulation.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Elekta's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

24. Plaintiff Carla Tracy is a resident and citizen of Dekalb, Illinois and brings this lawsuit on behalf of herself and all others similarly situated. Prior to the Data Breach, Plaintiff Tracy was a cancer patient receiving diagnostic and medical treatment at Northwestern. Plaintiff received a notice, dated June 25, 2021, informing her that her Sensitive Information related to her care and treatment at Northwestern had been compromised and stolen in a cyberattack on Elekta's database that contained her Sensitive Information.

25. Plaintiff Darryl Bowsky is a resident and citizen of Chicago, Illinois and brings this lawsuit on behalf of himself and all others similarly situated. Prior to the Data Breach, Plaintiff Bowksy was a cancer patient receiving diagnostic and medical treatment at Northwestern. In coordination with his treatment, Plaintiff Bowksy also participated in a clinical trial wherein his DNA was submitted, analyzed and stored by Northwestern. Plaintiff received a notice, dated June 25, 2021, informing him that his Sensitive Information related to his care and treatment at Northwestern had been compromised and stolen in a cyberattack on Elekta's database that contained his Sensitive Information.

26. Plaintiff Deborah Harrington is a resident and citizen of Oak Park, Illinois and brings this lawsuit on behalf of herself and all others similarly situated. Prior to the Data Breach, Plaintiff Harrington was a cancer patient receiving diagnostic

and medical treatment at Northwestern. Plaintiff received a notice, dated June 25, 2021, informing her that her Sensitive Information had been compromised and stolen in a cyberattack on Elekta's database that contained her Sensitive Information.

27. Defendant Elekta is a Swedish radiation therapy, radiosurgery and related equipment and data services provider with its United States principal place of business located in Dunwoody, Georgia.

28. Defendant Northwestern is an Illinois Non-Profit corporation and integrated health system offering patients access to hundreds of locations including eleven hospitals throughout the Chicagoland area.[16] Northwestern was a medical provider and client of Defendant Elekta who acquired and stored Plaintiffs' and Class Members' Sensitive Information. Northwestern was also involved in active clinical research and clinical trials that gathered patient DNA to study genetic traits in cancer patients to help improve screening and treatment methods. One such study involved Plaintiff Bowsky.

FACTUAL BACKGROUND

29. Elekta was founded in 1972 in Stockholm, Sweden and is currently listed on the Nordic Exchange under the ticker "EKTAb" even though nearly half of the company's sales are in the United States. With approximately 4,300 employees

[16] https://www.nm.org/about-us/northwestern-medicine-newsroom/media-relations/about-our-health-system (last visited September 28, 2021).

worldwide, Elekta generates approximately $1.6 billion dollars in annual sales globally with approximately $365 million annually in the United States.

30. Twenty-five percent (25%) of Elekta's annual revenue is derived from its software services.[17] Elekta's software service business provides a "large stream of recurring revenues based on long-term service contracts" with its healthcare customers.

31. Elekta also provides "cloud based" solutions that are hosted on Elekta Axis, a fully managed services cloud environment built specifically for Elekta software to improve scalability and reliability.

32. The integrated software component helps provide "access to more timely and complete patient information." It provides "better tools for sharing, analyzing, and applying information", and provides for information guided care for cancer patients.[18] The Elekta system also provides the ability to "track and manage oncology treatments" including comprehensive and integrated oncology information system where the database "aggregates all of your patient data, clinical regimes, and pharmacy information".[19]

33. Recognizing that the treatment of cancer is "complex and data driven,"

[17] https://www.elekta.com/investors/fileadmin/reports/annual-reports/elekta-annual-report-2020-21-en.pdf at pg. 18 (last visited July 14, 2021).
[18] https://www.elekta.com/software-solutions/# (last visited Jan. 22, 2022).
[19] https://www.elekta.com/software-solutions/care-management/mosaiq-medical-oncology (last visited Jan. 22, 2022).

Elekta has seized on the big data and artificial intelligence healthcare market to increase its revenues. Elekta designed its oncology software to capture and leverage patient data with the goal of automating healthcare processes.

34. Without patient data to analyze and organize for medical practitioners, Elekta's software is of no value; it is the complete and comprehensive data provided exclusively by Plaintiffs and Class Members that creates the billion-dollar value of the Elekta system.

35. Elekta's value is based on its ability to store and organize the patients' Sensitive Information, which then allows the health care providers a more comprehensive platform to analyze the data with the additional goal of improving both clinical outcomes and improve the financial performance of the healthcare provider. For example, the database assists Northwestern in compiling and organizing the extensive patient Sensitive Information required for mandatory reporting under Illinois law.

36. Recognizing the highly competitive and regulated healthcare industry in the U.S., Elekta claims to maintain "[s]ound practices for risk management" which "are an essential element of our culture, corporate governance, strategy development, and operational and financial management."[20] In turn, Elekta has established an Enterprise Risk Management (ERM) framework to provide guidance on governance,

[20] *Id*. at 34.

risk management and internal controls.[21]

37. Elekta recognizes the operational risk of a cyber security breach, that there needs to be an "appropriate measure to protect the data against damage,"[22] and that there is "an increasing threat of material cyber and information security attacks targeting healthcare data."[23] Yet, despite being on notice and fully aware of the risks, Defendants failed to adequately secure Plaintiffs' and Class Members' Sensitive Information.

38. As detailed more fully below, Elekta failed to safely and securely store the Sensitive Information entrusted to it and failed to prevent it from being compromised during the Data Breach.

39. As a condition of engaging in health services and/or clinical trials, Defendant Northwestern requires that its patients and clinical trial participants entrust them with Sensitive Information. The Sensitive Information is subsequently shared with its vendor and agent Elekta for reporting requirements with the State of Illinois. Upon information and belief, the Sensitive Information that is gathered and utilized during the care and treatment of cancer patients is also shared and utilized on the Elekta platform to help coordinate patient care including assisting in the regular course of medical care and with the practice of precision medicine (also referred to as

[21] *Id.*
[22] *Id.* at 35.
[23] *Id.* at 98.

precision oncology).

40. The field of cancer diagnostics is evolving "as a result of the rapid discovery of new genes associated with cancer, improvements in laboratory techniques for identifying disease causing events, and novel analytic methods that enable the integration of many different types of data." [24]

41. Precision medicine has changed the nature of treatment for cancer patients.[25] Precision medicine is an approach to cancer treatment in which the diagnosis and treatment are specifically tailored to the genes, proteins, and other substances in the patient's body. [26]

42. Precision oncology, defined as molecular profiling of tumors to identify targetable alterations, has entered the mainstream of clinical practice. The goal of precision medicine is simply to deliver the right cancer treatment to the right patient at the right dose and the right time. [27]

43. Elekta brands itself as a leader in "Precision Radiation" and informs its investors that "[a]dvancements in the ability to act on genetic, diagnostic and patient reported information means care can become more personalized. This requires

[24] https://www.bmj.com/content/350/bmj.h1832.long (last visited Feb. 1, 2022)
[25] https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2786987
[26] https://www.cancer.gov/about-cancer/treatment/types/biomarker-testing-cancer-treatment#:~:text=A%20biomarker%20test%20may%20be,those%20you%20are%20born%20with.
[27] https://ascopubs.org/doi/full/10.1200/EDBK_174176 (last visited Feb. 1, 2022)

treatment solutions and systems that are better and more precise. In the field of information systems, Elekta integrates data-driven recommendations, in which details about a patient's health and disease are combined with information used to optimize the treatment sessions."[28]

44. Genetic tests look for changes in a person genes or changes in the amount, function or structure of key proteins coded by specific genes. Genetic tests can look at the DNA or RNA that play a role in certain conditions. [29]

45. There are a wide variety of genetic based tests available to assist physicians in diagnosing and developing a personalized and targeted treatment plan for cancer patients. The broad categories include: hereditary genetic testing, biomarker genetic testing, and neo genomic sequencing. The test results are often used by practitioners to predict which patients are likely to have a better or worse outcome or respond to specific types of medication, chemotherapy and radiation treatment.

46. Hereditary genetic testing involves looking for specific inherited mutations or changes (variants) in a person's genes. This type of genetic test is commonly administered in patients when a cancer was diagnosed at an usually young

[28] https://www.elekta.com/investors/fileadmin/reports/annual-reports/elekta-annual-report-19-en.pdf (pg. 11) (last visited Feb. 1, 2022).
[29] http://encyclopedia.nm.org/Conditions/Cancer/Genetics/85,p07370 (last visited Feb. 1, 2022)

age, unusual type of cancer (e.g., breast cancer in a male), patient is diagnosed with several different types of cancer, or if multiple family members present with the same type of cancer (e.g., ovarian cancer). [30] Tests for cancer susceptibility genes are usually done by DNA studies. [31]

47. Hereditary testing for BRCA 1 or BRCA 2 gene, which is a simple blood test, has become an integral part of clinical care for patients with breast and ovarian cancer. [32] These tests are often administered where two or more first degree relatives (parents, sibling or child) have been diagnosed with breast or ovarian cancer. In addition, active breast cancer patients often elect this type of genetic test when considering different surgical treatment options.

48. Genetic hereditary testing is also commonly performed in active prostate cancer and colorectal cancer patients to select surgical and medication options. For example, the FDA has approved two medications, rucaparib and Olaparib, that are limited to patients with certain genetic mutations, due to the efficacy of the medication. Consequently, genetic testing is necessary on these patients to determine qualification for the treatment. [33]

---

[30] https://www.cancer.gov/about-cancer/causes-prevention/genetics/genetic-testing-fact-sheet#what-is-genetic-testing (last visited Feb. 1, 2022)
[31] http://encyclopedia.nm.org/Search/85,p07370 (last visited Feb. 1, 2022)
[32] https://ascopubs.org/doi/full/10.1200/JCO.18.01854 (cohort study of 77, 085 breast cancer patients showed that 24.1% had hereditary genetic tests performed)(last visited Feb.2, 2022)
[33] https://www.pcf.org/news/new-recommendations-offer-guidance-for-clinicians-

49. Some cancer treatments including targeted therapies and immunotherapies, may only work with certain biomarkers. Biomarker testing (also known as tumor genetic testing) is a different type of genetic test than hereditary genetic testing. Biomarker testing involves testing a sample of the cancer cells to identify genetic markers. During biomarker testing, the health care provider will look for genes, proteins, and other substances or tumor marks that provide information about the cancer.

50. The most well-known example is HER2 positive breast cancer, where patients do not respond as well to certain chemotherapy drugs. But newer drugs such as Herceptin have been specifically designed to attack HER2 positive cancers. Breast cancers, therefore, are routinely genetically tested to identify which patients will benefit from these drugs.[34]

51. Neo-genomics sequencing (also known as Next-generational sequencing or DNA Sequencing) is commonly utilized in precision oncology to uncover genetic alterations or mutations that are causing the cells to malfunction and develop the cancer. [35] Types of genetic test include flow cytometry, FISH, cytogenics, and

---

patients-on-implementing-genetic-testing-for-prostate-cancer/ (last visited Feb. 2, 2022)

[34] *Id.*

[35] https://www.webmd.com/cancer/cancer-genomes-21/what-is-genomic-testing#:~:text=Genomic%20testing%20is%20one%20method,rather%20than%20a%20specific%20one (last visited Feb. 1, 2022)

targeted or broad paneled DNA and RNA next-generational sequencing. Next-generation sequencing has become the primary tool in precision oncology to characterize an individual's tumor. [36]

52. A patient's medical history includes the test results ordered by the physician. This would include hereditary genetic testing results, biomarker genetic testing results, and neo-genomic sequencing results. A patients' medical history would also include the elected and prescribed therapy and response to the prescribed treatment.

53. There are also many clinical trials that acquire genetic information as part of the study. Plaintiff Bowsky was recruited and participated in one such study where his genetic information and DNA was provided to Northwestern. Upon information and belief, the genetic testing results would also be included in his medical history records.

A. **The Data Breach**

54. As a major component of its oncology and neuroscience business, Elekta maintains large volumes of its clients' Sensitive Information. As such, Elekta is well aware of the value of healthcare patient data which is highly sought by cybercriminals.

55. Elekta sells itself as able to "[p]rotect your data" with improved data

[36] https://neogenomics.com/diagnostic-services/methodologies/ngs (last visited Feb. 1, 2022)

security and AI along with multi-layer threat protection, better data organization leveraging modular infrastructure and disk encryption at rest.[37] Elekta "ensures that safeguarding your clinical data is our highest priority."[38]

56. Yet, while its customers reasonably believed their patient data was safe within Elekta's confines, in April 2021, Elekta allowed cyber criminals to infiltrate Elekta's data infrastructure's security walls.

57. In late April 2021, Elekta was the subject of a ransomware attack that targeted its cloud-based systems, maintaining oncology and radiology data, including that of Plaintiffs and Class Members. Included in the ransomware attack was the PII and PHI provided to Elekta by certain of its oncology and radiology healthcare clients. Shortly thereafter, Elekta began emailing its clients that it was taking action to immediately cut off the cyberattackers by temporarily taking its systems offline and cancelling or rescheduling radiation treatment appointments for cancer patients.

58. Soon after the breach notification, an Elekta representative explained:

> Elekta was subjected to a series of cyberattacks which affected a subset of U.S.-based customers on our first-generation cloud system. On April 20, to contain and mitigate the attacks, Elekta proactively took down its first-generation cloud system in the United States. An investigation is being conducted, and any affected customer(s) will be contacted and fully briefed through the appropriate channels and in accordance

[37] https://www.elekta.com/software-solutions/cloud-solutions/ (last visited Jan. 22, 2022).
[38] *Id.*

with any legal requirements.[39]

59. As a result of the Data Breach, many cancer patients across the United States had their cancer treatment delayed or disrupted when Elekta decided to temporarily take its system offline to protect any further exfiltration of patient and its customer's information.

60. In late May 2021, Elekta began notifying its healthcare clients that their clinical information containing the PII and PHI of patients may have been compromised in the ransomware Data Breach.

61. Elekta's healthcare clients then began notifying their patients, including Plaintiffs and Class Members. For example, in June 2021, Northwestern Memorial HealthCare notified approximately 201,197 patients that "an unauthorized individual gained access to [Elekta's] systems between April 2, 2021 and April 20, 2021 and, during that time, acquired a copy of the database that stores some oncology patient information."[40] Additionally, on or about June 25, 2021, Renown Health notified approximately 65,181 patients that "[w]e are writing to inform you of a recent data security incident that involved our business associate, Elekta, Inc. ('Elekta')."[41]

[39] https://compliancy-group.com/healthcare-vendor-ransomware-attack-170-health-systems-hit/ (last visited Jan. 22, 2022).
[40] https://www.nm.org/patients-and-visitors/notice-of-privacy-incident (last visited July 14, 2021)
[41] file:///C:/Users/nprosser/Downloads/Elekta_Media-Notice%20(1).pdf (last visited July 14, 2021)

62. Additional data breach notifications went out to other Elekta clients such as Cancer Centers of Southwest Oklahoma, Carle Health, Lifespan, Charles Health System, Yale New Haven Health, Emory Healthcare and Southcoast Health. In total, approximately 42 healthcare systems are believed to have been affected by the Data Breach that happened on Elekta's watch.

63. The various data breach notices have indicated the stolen PII and PHI included full names, Social Security numbers, addresses, dates of birth, height, weight, medical diagnoses, medical treatment details, appointment confirmations, and other personal and protected information. Specifically, Plaintiffs' notices indicated the data involved in the Data Breach "may have included patient names, dates of birth, Social Security numbers, health insurance information, medical record numbers, and clinical information related to cancer treatment, such as medical histories, physician names, dates of service, treatment plans, diagnoses, and/or prescription information."

64. The Northwestern Notice letter was also specific about the purpose of the database that was accessed. This Elekta database was being utilized for complying with mandatory cancer reporting requirements with the State of Illinois.[42]

65. Illinois has specific requirements in terms of the type of information that must be reported related to cancer patients. Specifically, Northwestern was required to provide abstracts in seven different categories with information contained in the

[42] Ex. 1. Northwestern Breach Notice Letter

patient's medical records, including the following:

- *Reporting Information* – type of report being submitted, abstracter identification code and the date the abstract was submitted.

- *Patient Data and Resident Address* − patient's full name (including maiden name, when applicable and available), Social Security number, telephone number, and residential address, including street address, city, county, state, and postal code.

- *Personal Data* − patient's birthdate, age, sex, race, ethnicity, marital status, birthplace, history of tobacco and alcohol usage, history of occupation and industry, health insurance status and socio-economic status including, but not limited to, education and income.

- *Diagnosis Data* − initial diagnosis date; diagnostic information; method of diagnosis; primary site; laterality; histology and behavior code; grade; stage of disease, including clinical and pathological extent of disease information; existence of other reportable primary diseases and date of diagnosis; first course cancer-directed therapy; and supporting text information for all diagnostic procedures, histology, primary site, staging and treatment.

- *Facility Data* − facility identification number provided by the Department of Public Health, the medical record number, date of admission, type of reporting source, accession number (if available), case identification type, discharge date and status, class of case, and name and Illinois medical license number of attending physician.

- *Follow-Up Data* − date of last follow-up or death, follow-up status, type of follow-up, names of follow-up physicians, cause of death, whether patient information is incomplete, and names and Illinois medical license numbers of managing and treating physicians.

- *Text Documentation* – description of the primary site, histology, diagnostic test results, staging, pathology results and treatment information.[43]

66. As such, the scope and type of Sensitive Information that would have plausibly been included in the compromised Elekta reporting database would have included all of the types of data necessary to comply with the mandatory Illinois reporting requirements.

67. While PGI and DNA data has not been confirmed or specifically disclosed at this time by Defendants as part of the breach, the Data Breach involves a database that was designed to assist Northwestern with detailed state reporting requirements that included "clinical and pathological extent of disease information", "supporting text for all diagnostic procedures", as well as "histology, diagnostic test results, staging, pathology results, and treatment information." Genetic testing and DNA analysis whether in the form of biomarker testing, gene expression panels, hereditary testing, or other forms of genetic testing and evaluation, all fall within these broad categories of medical information that Northwestern was required to provide to the State. Elekta was storing and organizing this type of information to assist with Northwestern's reporting obligation.

68. Genetic testing and DNA analysis, whether in the form of biomarker testing, gene expression panels, hereditary testing, or other forms of genetic testing

[43] *Id.*

and evaluation, also all fall within the broad category of "clinical information related to your cancer treatment", "medical history", "treatment plan", "diagnosis and/or prescription information" that Northwestern disclosed in its Breach Notice Letter to its patients.

69. This Data Breach involved a broad and extensive breach of Elekta's cloud-based system that was specifically designed to contain comprehensive and complete medical information involving cancer patients, including Plaintiffs.

70. Upon information and belief, the Data Breach included genetic testing and DNA analysis such as Biomarker testing, gene expression panels, hereditary testing, or other forms of genetic testing data that had been was either (a) being utilized for cancer patient care planning through the Elekta system and/or (b) being stored and organized through the Elekta system to comply with State Cancer reporting requirements.

B. Data Breaches Lead to Identity Theft and Cognizable Injuries.

71. The personal, health, and financial information of consumers, such as Plaintiffs and Class Members, is valuable and has been commoditized in recent years.

72. Defendants were at all times fully aware of its obligations to protect the Sensitive Information of consumers because of its business model of collecting Sensitive Information and storing such information for analysis and for pecuniary gain. Defendants were also aware of the significant repercussions that would result

from its failure to do so.

73. Elekta knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security were breached. Elekta failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

74. PII and PHI are valuable commodities to identity thieves, particularly when it is aggregated in large numbers when multiple types of information for a single user are combined. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical or financial fraud.

75. Elekta specifically clearly recognizes the operational risk and notes that there needs to be an "appropriate measure[] to protect the data against damage,"[44] and further expounds that there is "an increasing threat of material cyber and information security attacks targeting healthcare data."[45]

76. Elekta sells itself as able to "[p]rotect your data" with improved data security and AI along with multi-layer threat protection, better data organization leveraging modular infrastructure and disk encryption at rest.[46] Elekta "ensures that

[44] https://www.elekta.com/investors/fileadmin/reports/annual-reports/elekta-annual-report-2020-21-en.pdf at pg. 35 (last visited July 14, 2021)
[45] *Id.* at 98.
[46] https://www.elekta.com/software-solutions/cloud-solutions/ (last visited Jan. 23, 2022).

safeguarding your clinical data is our highest priority."[47]

77. The medical community and Defendant Northwestern are aware of numerous recent data breaches on medical facilities and their vendors.

78. In May 2019, the American Medical Collection Agency (AMCA) reported that an 8-month data breach had exposed more than 20 million patients' Sensitive Information. This event brought into focus the risk faced when healthcare providers work with outside vendors and allow access to their systems.

79. According to the United States Cybersecurity & Infrastructure Security Agency:

> Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.[48]

80. Since these warnings, healthcare-related breaches have continued to rapidly increase, and yet Defendants failed to exercise the reasonable care in hiring, training, and supervising their employees and agents to implement necessary data security and protective measures.

---

[47] *Id.*

[48] https://www.cisa.gov/ransomware (last visited Apr. 16, 2021).

81. As such, Defendants should have not only known about the potential for the data breach but should have taken steps to increase the security. Instead, they relied on their outdated data security safeguards leading to the Data Breach.

82. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as a person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

83. Stolen PII and PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

84. Once PII and PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

85. According to the FBI's Internet Crime Complaint Center (IC3) 2020 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $4.1 billion in losses to

individuals and business victims.[49]

86. In 2020, as the COVID-19 global pandemic permeated all aspects of life, cyber fraudsters took the opportunity to exploit the pandemic and targeted both businesses and individuals.[50] As healthcare systems experienced an unprecedented challenge of grappling with the varying components and effects of COVID-19, a major ramification also was exploited by the increase in data breaches to patient data.[51]

87. In addition to the exposure directly related to data breaches involving PII and PHI effectuated through the healthcare system, victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opening accounts or misuse of existing accounts.

88. Data breaches facilitate identity theft as hackers obtain consumers' PII and PHI, thereafter using it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII and PHI to others who do the same.

89. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming

---

[49] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Jan. 22, 2022).
[50] *Id.*
[51] https://www.prnewswire.com/news-releases/health-data-breaches-skyrocket-during-covid-19-pandemic-301247097.html (last visited July 14, 2021).

the many obstacles they face in obtaining or retaining credit.

90. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, many victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

91. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII and PHI. To protect themselves, Plaintiffs and Class Members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

92. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

93. Recognizing the high value consumers place on their PII and PHI, many companies now offer consumers an opportunity to sell this information to advertisers

and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[52]

94. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of same. Research shows how much consumers value their data privacy, and the amount is considerable.

95. By virtue of the Data Breach here and unauthorized release and disclosure of the PII and PHI of Plaintiffs and the Class, Defendants have deprived Plaintiffs and Class Members of the substantial value of their PII and PHI, to which they are entitled. As previously alleged, Defendants failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

96. According to the FTC, unauthorized PII and PHI disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[53]

---

[52] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last accessed Jan 22, 2022).

[53] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last accessed Jan. 22, 2021).

97. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

98. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

99. As a direct and proximate result of Defendants' wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiffs' and other Class Members' PII and PHI, Plaintiffs and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are

entitled to compensation; and (iii) out-of-pocket expenses for securing identity theft protection and other similar necessary services.

C. FTC Guidelines Prohibit Unfair or Deceptive Acts

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

101. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[54]

102. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[55]

103. The FTC further recommends that companies not maintain PII longer

[54] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 22, 2022).
[55] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf (last visited Jan. 22, 2022).

than is needed for authorization of a transaction; limit access to private 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.[56]

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

105. Elekta failed to properly implement basic data security practices. Elekta's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

106. Elekta was at all times fully aware of its obligations to protect the PII and PHI of consumers because of its business model of collecting PII and PHI and storing such information for analysis and for pecuniary gain. Elekta was also aware of the significant repercussions that would result from its failure to do so.

D. Privacy was an Integral Part and Reasonable Expectations of the Services Provided

[56] *Id.*

107. Confidentiality is a cardinal rule of the provider-patient relationship.

108. Plaintiffs and Class Members are aware of a medical provider's duty of confidentiality, and as a result, have an objective reasonable expectation that Northwestern will not share or disclose, whether intentionally or unintentionally, Sensitive Information in the absence of authorization for any purpose that is not directly related to or beneficial to patient care.

109. Likewise, pursuant to HIPAA and industry standards, medical providers understand that the services they provide to patients includes confidentiality.

E. HIPAA Standards & Violations

110. Upon information and belief, Defendants each failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of its customers' personal information in compliance with industry recognized cybersecurity framework and HIPAA.

111. The Data Breach resulted from a combination of insufficiencies that indicate the Defendants failed to comply with safeguards mandated by Federal and State Law and industry standards. The security failures included but are not limited to:

A. Failing to maintain an adequate security system to prevent data loss;

B. Failing to implement policies and procedures that limit use and disclosure of PII and PHI to its vendors to the minimum necessary;

C. Failing to mitigate the risks of data breach and loss of data;

D. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit in violation of 45 C.F.R. 164. 306(a)(1);

E. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access to only those persons or software programs that have been granted access 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 violations of 45 C.F.R 164.308(a)(1);

G. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

H. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

I. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5);

J. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c); and,

K. Releasing, transferring, allowing access to, and divulging protected Sensitive Information to unauthorized criminal third parties.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

112. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if their data security, or agent's data security systems were breached, including the significant costs that would be imposed on Plaintiffs and the Class as a result of the breach.

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

114. As a result of the Breach, Plaintiffs and the other Class Members must now be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. The need for additional monitoring for identity theft and fraud will extend indefinitely into the future.

115. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once

had in the financial community.

116. Plaintiffs and the other Class Members have suffered and will suffer actual injury due to loss of time and increased risk of identity theft as a direct result of the Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiffs and the other Class Members suffer ascertainable losses in the form of out-of-pocket expenses, opportunity costs, and the time and costs reasonably incurred to remedy or mitigate the effects of the Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of the Defendants;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring health insurance, medical information, financial accounts and credit reports for unauthorized activity for years to come.

117. Moreover, Plaintiffs and the other Class Members have an interest in ensuring that Defendants implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Sensitive Information, including making sure that the storage of data or documents containing Sensitive Information is not accessible by unauthorized persons and that access to such data is sufficiently protected.

118. Furthermore, Plaintiffs and the Class Members did not receive the value of the bargain for the medical services that were paid for, which included an agreement to keep their medical information private and confidential as part of the care and treatment.

119. And finally, as a direct and proximate result of Defendants' actions and inactions, Plaintiffs and the other Class Members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future

harm.

In addition to the remedy for economic harm, Plaintiffs and the Class Members maintain an undeniable and continuing interest in ensuring that the Sensitive Information remains in the possession of Defendants is secure, remains secure, and is not subject to future theft.

120. Plaintiffs also are entitled to statutory damages under GIPA (410 ILCS 513.

CLASS DEFINITION AND ALLEGATIONS

121. Plaintiffs brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following classes:

The Nationwide Class:

> All persons residing in the United States who had their Sensitive Information hosted by Elekta compromised as a result of the Data Breach.

The Illinois Subclass:

> All persons residing in the State of Illinois who had their Sensitive Information hosted by Elekta compromised as a result of the Data Breach.

The Illinois GIPA Subclass:

> All persons residing in the State of Illinois who had PGI hosted by Elekta compromised as a result of the Data Breach.

Excluded from the Class and Subclass are: (i) Defendants and its officers, directors, affiliates, parents, and subsidiaries; (ii) the Judge presiding over this action; and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches.

122. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

123. The members of the Class and Subclasses are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class includes over 200,000 individuals who have been damaged by Defendants' conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendants' records.

124. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendants engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendants owed Plaintiffs and the other Class Members a

duty to adequately protect their Sensitive Information;

d. whether Defendants breached its duty to protect the Sensitive Information of Plaintiffs and the other Class Members;

e. whether Defendants knew or should have known about the inadequacies of their data protection, storage, and security;

f. whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class Members' Sensitive Information from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendants' computer systems and digital storage environment;

h. whether Defendants had the proper computer systems to safeguard and protect Plaintiffs' and the other Class Members' Sensitive Information from unauthorized theft, release or disclosure;

i. whether Defendants breached the promise to keep Plaintiffs' and the Class Members' Sensitive Information safe and to follow federal data security protocols;

j. whether Defendants' conduct was the proximate cause of Plaintiffs' and the other Class Members' injuries;

k. whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

l. whether Plaintiffs and the other Class Members suffered ascertainable and cognizable injuries as a result of Defendants' conduct;

m. whether Plaintiffs and the other Class Members are entitled to recover actual damages and/or statutory damages;

n. whether Plaintiffs and the other Class Members were intended third-party beneficiaries to the contracts between Defendant Elekta and its medical provider customers, such as Defendant Northwestern; and,

o. whether Plaintiffs and the other Class Members are entitled to other appropriate remedies, including injunctive relief.

125. Defendants engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the other Class Members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

126. Plaintiffs' claims are typical of the claims of the members of the Class and Subclass. All Class Members were subject to the Data Breach and had their Sensitive Information accessed by and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in a similar manner.

127. Plaintiffs will fairly and adequately protect the interests of the Members

of the Class, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Plaintiffs has no adverse or antagonistic interests to those of the Class.

128. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class Members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class and the Illinois Subclass)

129. Plaintiffs restate and reallege all proceeding factual allegations above and hereafter as if fully set forth herein.

130. Upon gaining access to the Sensitive Information of Plaintiffs and

Members of the Class, Defendants owed to Plaintiffs and the Class a common law duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendants were required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the Sensitive Information of Plaintiffs and the Class. Defendants further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

131. Defendants owed this duty to Plaintiffs and the other Class Members because Plaintiffs and the other Class Members compose a well-defined, foreseeable, and probable class of individuals whom Defendants should have been aware could be injured by Defendants' inadequate security protocols. Defendants actively solicited clients who entrusted Defendants with Plaintiffs' and the other Class Members' Sensitive Information when obtaining and using Defendants' services. To facilitate these services, Defendants used, handled, gathered, and stored the Sensitive Information of Plaintiffs and the other Class Members. Attendant to Defendants' solicitation, use and storage, Defendants knew of its inadequate and unreasonable security practices with regard to their computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII and PHI that

Defendants actively solicited from clients who entrusted Defendants with Plaintiffs' and the other Class Members' data. As such, Defendants knew a breach of its systems would cause damage to its clients and Plaintiffs and the other Class Members. Thus, Defendants had a duty to act reasonably in protecting the Sensitive Information of its healthcare clients' patients.

132. Defendants breached their duty to Plaintiffs and the other Class Members by failing to implement and maintain security controls that were capable of adequately protecting the Sensitive Information of Plaintiffs and the other Class Members.

133. Defendants also breached their duty to timely and accurately disclose to the clients, Plaintiffs and the other Class Members, that their Sensitive Information had been or was reasonably believed to have been improperly accessed or stolen.

134. Defendants' negligence in failing to exercise reasonable care in protecting the Sensitive Information of Plaintiffs and the other Class Members is further evidenced by Defendants' failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

135. Section 5 of the Federal Trade Commission Act ("FTCA") Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendants to take reasonable measures to protect Plaintiffs' and the Class Member's Sensitive Information data and is a further source of Defendant's duty to Plaintiffs and the Class

Members. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants of failing to implement and use reasonable measures to protect Sensitive Information. Defendants, therefore, were required and obligated to take reasonable measures to protect Sensitive Information it solicited, possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duty to adequately protect Sensitive Information. By failing to implement and use reasonable data security measures, Defendants acted in violation of § 5 of the FTCA.

136. Defendants are obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendants to exercise reasonable care with respect to Plaintiffs and the Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendants were the only entities of adequately protecting the data that that they alone solicited, collected, and stored.

137. The injuries to Plaintiffs and the other Class Members were reasonably foreseeable to Defendants because common law, statutes, and industry standards require Defendants to safeguard and protect their computer systems and employ

procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the other Class Members' PII and PHI.

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

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

140. Defendants' failure to take reasonable steps to protect the PII and PHI of Plaintiffs and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiffs' and the other Class Members' PII and PHI. This ease of access allowed thieves to steal PII and PHI of Plaintiffs and the other Class Members, which could lead to dissemination in black markets.

141. As a direct proximate result of Defendants' conduct, Plaintiffs and the other Class Members have suffered theft of their PII and PHI. Defendants allowed thieves access to Plaintiffs' and Class Members' PII and PHI, thereby decreasing the security of Plaintiffs' and Class Members' financial and health accounts, making Plaintiffs' and Class Members' identities less secure and reliable, and subjecting Plaintiffs' and Class Members to the imminent threat of identity theft. Not only will Plaintiffs and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

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

143. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, and punitive damages, in an

amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class and the Illinois Subclass)

144. Plaintiffs restate and reallege all proceeding factual allegations above and hereafter as if fully set forth herein.

145. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Elekta for failing to use reasonable measures to protect PII/PHI. Various FTC publications and orders also form the basis of Elekta's duty.

146. Defendant Elekta violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant Elekta's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of a data breach.

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

148. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

149. Defendant Elekta's unreasonable data security measures and failure to timely notify Plaintiffs and the Class of the Data Breach violates the Georgia

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

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

151. Defendant Elekta's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect Sensitive Information it required Plaintiffs and Class Members to provide and it stored constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

152. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes), the Georgia Constitution and the Restatement of the Law of Torts (Second), were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to

employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

153. As a direct and proximate result of Defendant Elekta's negligence, Plaintiffs and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
DEFENDANT NORTHWESTERN
***(*On Behalf of Plaintiffs and the Nationwide Class and the Illinois Subclass)**

154. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth here.

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

156. Plaintiffs and the Class were required to and delivered their Sensitive Information to Northwestern as part of the process of obtaining services provided by Northwestern. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

157. Northwestern accepted possession of Plaintiffs' and Class Members' Sensitive Information for the purpose of providing services or employment to

Plaintiffs and Class Members.

158. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Northwestern whereby Northwestern became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Sensitive Information.

159. In delivering their Sensitive Information to Northwestern and paying for healthcare services, Plaintiffs and Class Members intended and understood that Northwestern would adequately safeguard the data as part of that service.

160. In their written policies, Northwestern expressly promised to Plaintiffs and Class Members that it would only disclose protected information and other Sensitive Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

161. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

162. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII or PHI also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical

purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption from Bricker; and (6) other steps to protect against foreseeable data breaches.

163. Plaintiffs and the Class Members would not have entrusted their Sensitive Information to Northwestern in the absence of such an implied contract.

164. Had Northwestern disclosed to Plaintiffs and the Class that it would entrust such data to incompetent third-party agents that did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to Northwestern.

165. Northwestern recognized that Plaintiffs' and Class Members' personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

166. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Northwestern.

167. Northwestern breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their data as described herein.

168. As a direct and proximate result of Northwestern's conduct, Plaintiffs and

the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONTRACT – THIRD-PARTY BENEFICIARIES
DEFENDANT ELEKTA
(*On Behalf of Plaintiffs and the Nationwide Class and the Illinois Subclass*)

169. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

170. This count is brought on behalf of the Plaintiffs, the Nationwide Class and the Illinois Subclasses.

171. Upon information and belief, Plaintiffs, Class Members, and Subclasses Members are intended third-party beneficiaries of contracts entered into between Defendant Elekta and its customers, such as Defendant Northwestern and other similar medical providers.

172. Upon further information and belief, these contracts require, inter alia, that Elekta take appropriate steps to safeguard the Sensitive Information entrusted to it by Defendant Northwestern and other similar medical providers that obtain that information from Plaintiffs, Class Members, and Subclasses Members.

173. Plaintiffs, Class Members, and Subclasses Members are intended third-party beneficiaries of these contracts because these contracts are entered into for the purpose of storing Sensitive Information for persons such as Plaintiffs, Class Members

and Subclasses Members. Under these circumstances, recognition of a right to performance by Plaintiffs, Class Members, and Subclasses Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts, including Defendant Elekta, intended to give Plaintiffs, Class Members, and Subclasses Members the benefit of the performance promised in the contracts.

174. Defendant Elekta breached these agreements, which directly and/or proximately caused Plaintiffs, Class Members, and Subclasses Members to suffer substantial damages.

175. Upon information and belief, Defendant Elekta saved and/or avoided spending a substantial sum of money by knowingly failing to comply with its contractual obligations.

176. Therefore, Elekta has retained a benefit and been unjustly enriched while Plaintiffs, Class Members, and Subclass Members have been injured and are entitled to damages, restitution, and/or disgorgement of profits in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
VIOLATION OF ILLINOIS GENETIC INFORMATION PRIVACY ACT ("GIPA")
(410 ILCS 513)
*(*On Behalf of the Illinois GIPA Subclass*)*

177. Plaintiffs restate and reallege all proceeding allegations above and

hereafter as if fully set forth herein.

178. Genetic testing and genetic information are confidential and privileged and may only be released to the individual tested and to persons specifically authorized by that individual in writing.

179. Genetic information can be valuable to the individual and to criminal markets and includes the following:

A. Individuals' genetic tests;

B. The genetic tests of family members of the individual;

C. The manifestation of a disease or disorder in family members; and;

D. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, the individual or any family member or such individual. [57]

180. Genetic services means: (1) a genetic test; (2) genetic counseling (including obtaining, interpreting, or assessing genetic information); (3) or genetic education. [58]

181. Genetic testing means an analysis of human DNA, RNA, chromosomes, proteins or metabolites, if the analyses detect genotypes, mutations, or chromosomal changes.[59] This includes genetic tests that would be administered for BRCA1,

[57] 45 CFR 160.103
[58] *Id.*
[59] *Id.*

BRCA2, colorectal genetic variant, biomarker testing, neogenomics sequencing, Caris testing, and other genetic tests provided in a clinical setting to cancer patients.

182. Plaintiffs and Class Members allowed for genetic information derived from genetic testing to be acquired by and stored at Northwestern with the expectation that the genetic test results and genetic information would not be disclosed without consent.

183. Upon information and belief, such genetic information was contained within cloud systems that were hosted by Defendant Elektra and subject to the Data Breach at issue.

184. Defendants Elekta and Northwestern violated this act by negligently and recklessly disclosing the genetic information to criminal third parties as described herein by releasing, transferring, providing access to, divulging through its affirmative negligent actions and omissions Plaintiffs and Class Members Genetic Information to criminal third parties outside the entity.

185. As a direct and proximate result of the unauthorized disclosure of Plaintiff and Class Members genetic information, Plaintiff and the Class have suffered actual damages as described herein and liquidated damages under 410 ILCS 513.40.

SIXTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class and the Illinois Subclass)

186. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

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

188. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Sensitive Information, including whether Elekta is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Sensitive Information. Plaintiffs allege that Elekta's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Sensitive Information and remains at imminent risk that further compromises of their Sensitive Information will occur in the future.

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

a. Elekta owes a legal duty to secure consumers' Sensitive Information and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

b. Elekta breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Sensitive Information.

c. Elekta's breach of its legal duty continues to cause harm to Plaintiffs and the Class Members.

190. This Court also should issue corresponding injunctive relief requiring Elekta to employ adequate security protocols consistent with law and industry standards to protect consumers' (Plaintiffs' and the Class Members') Sensitive Information.

191. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Elekta. The risk of another such breach is real, immediate, and substantial. If another breach at Elekta occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class Members.

192. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Elekta if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On

the other hand, the cost to Elekta of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Elekta has pre-existing legal obligations to employ such measures.

193. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Elekta, thus eliminating the additional injuries that would result to Plaintiffs, Class Members and consumers whose Sensitive Information would be further compromised.

SEVENTH CAUSE OF ACTION
VIOLATION OF O.C.G.A. § 13-6-11
*(*On Behalf of Plaintiffs and the Nationwide Class and the Illinois Subclass*)*

194. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth here.

195. Defendants through their actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused Plaintiffs and Class Members unnecessary trouble and expense with respect to the events underlying this litigation.

196. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to implement and use reasonable measures to protect Sensitive Information. Various FTC publications and orders also form the basis of Defendants' duty.

197. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information that they obtained and stored and the foreseeable consequences of a data breach.

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

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

200. Defendants' implementation of inadequate data security measures, their failure to resolve vulnerabilities and deficiencies, and their abdication of its responsibility to reasonably protect data they required Plaintiffs and Class Members

to provide and stored on their own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

201. Defendants knew or should have known that they had a responsibility to protect the Sensitive Information they required Plaintiffs and Class Members to provide and stored, that they were entrusted with this Sensitive Information, and that they were the only entities capable of adequately protecting the Sensitive Information.

202. Despite that knowledge, Defendants abdicated their duty to protect the Sensitive Information they required Plaintiffs and Class Members provide and that they stored.

203. As a direct and proximate result of Defendants' actions, Plaintiffs' and the Class Members' Sensitive Information was stolen. As further alleged above, the Data Breach was a direct consequence of Elekta's abrogation of data security responsibility and their decision to employ knowingly deficient data security measures that knowingly left the Sensitive Information unsecured. Had Elekta adopted reasonable data security measures, it could have prevented the Data Breach.

204. As further described above, Plaintiffs and the Class Members have been injured and suffered losses directly attributable to the Data Breach.

205. Plaintiffs and Class Members therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that

the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

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

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

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

c. For damages in an amount to be determined by the trier of fact;

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

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses pursuant to O.C.G.A. § 13-6-11 and as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded: and

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

DEMAND FOR JURY TRIAL

Plaintiffs Carla Tracy, Darryl Bowsky, and Deborah Harrington, on behalf of themselves individually and the putative Class, demand a trial by jury on all claims so triable.

Respectfully Submitted,

THE FINLEY FIRM, P.C.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Fax: (404) 320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Plaintiffs' Liaison Counsel

Bryan L. Bleichner*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Ste. 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

Terence R. Coates*
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219

tcoates@msdlegal.com

Interim Co-Lead Counsel

Joseph M. Lyon**
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Nathan D. Prosser*
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
Fax: (952) 941-2337
nprosser@hjlawfirm.com

Gary M. Klinger*
MASON LIETZ & KLINGER, LLP
227 W. Monroe Street, Ste. 2100
Chicago, IL 60606
Tel: (202) 975-0477
gklinger@masonllp.com

Todd S. Garber*
Andrew C. White*
FINKLESTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Seth A. Meyer*
Alex J. Dravillas *
KELLER LENKNER LLC

150 N. Riverside, Suite 4270
Chicago, IL 60606
Tel : (312) 741-5220
sam@kellerlenkner.com
ajd@kellerlenkner.com

Mara Baltabols*
FISH POTTER BOLANOS, P.C.
200 e. 5 th Ave., Suite 123
Naperville, IL 60563
Tel : (630) 364-4061
mbaltabols@fishlawfirm.com

Plaintiffs' and Putative Class Counsel

**Pro Hac Vice*
*** Pro Have Vice Forthcoming*

CERTIFICATE OF SERVICE & COMPLIANCE

I hereby certify that on this date I served the foregoing **Consolidated Amended Class Action Complaint** via the CM/ECF system, which will automatically provide-email notification and service of such filing to counsel of record for all parties registered with the Court for electronic filing, as follows:

Gregory T. Parks
MORGAN, LEWIS & BOCKIUS LLP
1701 Market Street
Philadelphia, PA 19103
Tel: (215) 963-5000
Fax: (215) 963-5001
gregory.parks@morganlewis.com
Counsel for Defendants, Elekta, Inc., and Northwestern Memorial Healthcare

Michael A. Caplan
Cameron B. Roberts
CAPLAN COBB LLP
75 14th Street NE, Suite 2750
Atlanta, Georgia 30309
Tel: (404) 596-5600
Fax: (404) 596-5604
mcaplan@caplancobb.com
croberts@caplancobb.com
Counsel for Defendant, Elekta, Inc.

This 2nd day of February, 2022.

I further certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON