JUDGE DAVID KEENAN

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

JANICE BUSBY RICHARDSON, individually and on behalf of others similarly situated, Plaintiffs, v. OVERLAKE HOSPITAL MEDICAL CENTER AND OVERLAKE MEDICAL CLINICS, LLC, Defendants.	Cause No. 20-2-07460-8 SEA **AMENDED CLASS ACTION COMPLAINT**

I. AMENDED CLASS ACTION COMPLAINT

Plaintiff, Janice Busby Richardson, individually, and on behalf of all others similarly situated, brings this action against Defendants, Overlake Hospital Medical Center and Overlake Medical Clinics, LLC, (collectively, "Defendants" or "Overlake") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

II. JURISDICTION AND VENUE

2.1 Jurisdiction is proper in this Court because the principal place of business for each of the Defendants is in King County, Washington.

2.2 Venue is proper in this Court as a substantial portion of the acts and transactions

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

that constitute violations of law complained of herein occurred in King County and Defendants conduct substantial business throughout King County.

III. NATURE OF THE ACTION

3.1 This class action arises out of the recent cyberattack and data breach ("Data Breach") at Defendants' medical facilities. As a result of the Data Breach, Plaintiff and approximately 109,000 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendants—was compromised and unlawfully accessed due to the Data Breach. Information compromised in the Data Breach includes names, demographic information, dates of birth, identification card numbers, health insurance information, medical information, other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendants collected and maintained (collectively the "Private Information").

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

3.3 Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

3.4 In addition, Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored their property, they would have discovered the intrusion sooner.

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

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

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

3.8 Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

3.9 Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

3.10 Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Overlake's data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

IV. PARTIES

4.1 Plaintiff Janice Busby Richardson is, and at all times mentioned herein was, an individual citizen of the State of Washington residing in the City of Kirkland.

4.2 Defendant Overlake Hospital Medical Center is a hospital and health system with its principal place of business at 1035 116th Ave. NE, Bellevue, WA, 98004.

4.3 Defendant Overlake Medical Clinics, LLC is a Washington limited liability company in the business of healthcare with its principal place of business at 1035 116th Ave. NE, Bellevue, WA, 98004.

V. DEFENDANTS' BUSINESS

5.1 Defendants render healthcare services, medical care, and treatment to the Puget Sound region throughout the State of Washington.

5.2 Defendants operate a 349-bed medical center offering a full range of advanced medical services. In addition, Defendants operate primary care clinics, urgent care clinics, specialty clinics, and an emergency and trauma center. It is accredited by the Healthcare Facilities Accreditation Program and has a Level III trauma center.

5.3 Defendants employ nearly 3,000 people and have some 1,000 active and courtesy providers on their medical staff, including more than 200 providers who are employed by the organization.

5.4 Defendants provide medical care, treatment, and attendant services in this non-exhaustive list of areas: cardiovascular, cancer treatment, birthing, surgery, intensive coronary care, rehabilitation, orthopedics, sports medicine, joint replacement, laboratory services, imaging, social services, cardiopulmonary, kidney dialysis, emergency room care, a sleep center, dermatology, E.N.T. and hearing, and women and children's care.

5.5 In the ordinary course of receiving treatment and health care services from Overlake, patients are required to provide sensitive personal and private information such as:

- Name, address, phone number and email address;

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information; and
- Other information that may be deemed necessary to provide care.

5.6 Prior to receiving care and treatment from Overlake, Plaintiff provided her name, address, phone number and email address; date of birth; demographic information (including her race and gender); Social Security number; information relating to her individual medical history; her insurance information and coverage; the names of her other doctors, nurses or other medical providers; photo identification, and; her employer information.

5.7 Overlake also gathers certain medical information about patients and create records of the care they provide to them.

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

5.9 All of Overlake's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes without a written authorization, as disclosed in the Overlake's Notice of Privacy Practices (the "Privacy Notice").[1] The current privacy notice has an effective date of June 13, 2018.

[1]https://www.overlakehospital.org/patient-notice-of-privacy-practices.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

5.10 The Privacy Notice is provided to every patient upon request and is posted on Overlake's website.

5.11 Because of the highly sensitive and personal nature of the information Overlake acquires and stores with respect to their patients, Overlake promises to, among other things: (A) "maintain the privacy of your health information"; (B) ""protect[] medical information about you"; (C) "follow the information practices that are described in this notice"; and (D) to not "use or disclose" patient health information "except as indicated in this notice."[2]

5.12 Upon information and belief, Overlake uses a portion of the payments made by its patients, or a portion of the payments made on behalf of its patients, to fund all of its data security, and does not have any separate or dedicated source of funding for any data security systems, procedures, or measures that Overlake employs.

VI. THE CYBERATTACK AND DATA BREACH

6.1 On December 9, 2019, Overlake learned that an unauthorized person or persons gained access to Overlake company email accounts between December 6-9, 2019.[3]

6.2 The cyberattack began on December 6, 2019, three days prior to Defendants' discovering the data breach on December 9, 2019, and giving the cybercriminals three full days of unfettered access to at least one employee email account of Defendants that contained highly confidential and protected patient information.

6.3 The cybercriminals spread their attack out to encompass additional employee email accounts that were compromised for multiple hours on Dec. 9, 2019. Those additional employee email accounts also contained highly confidential and protected patient information.

6.4 After discovery of this incident, Defendants began an investigation of the fallout from the cyberattack.

6.5 The email accounts accessed by the Data Breach included one or more of the

[2] *Id*.

[3] https://www.overlakehospital.org/sites/default/files/inline-files/notice-of-phishing-incident.pdf.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

following: names, demographic information, dates of birth, identification card numbers, health insurance information, medical information, other protected health information as defined HIPAA, and additional PII and PHI.

6.6 The compromised email accounts contained messages and email attachments that included the Private Information of at least 109,000 patients, including Plaintiff's Private Information.

6.7 Based upon the notice she received from Defendants, Plaintiff believes her Private Information was stolen (and subsequently sold) in the Data Breach. Indeed, Overlake directly acknowledged that "unauthorized access to patient information may have occurred."[4]

6.8 Despite acknowledging that data thieves likely accessed Plaintiff's and the Class Members' Private Information, Defendants did not begin to notify affected patients until February 7, 2020, nearly two months after the data breach was discovered. *See* Notice of Phishing Incident, attached hereto as Exhibit 1.

6.9 Washington's Data Breach Notification law required Defendants to give notice "immediately following discovery," unless there is a pending law enforcement action that would be impeded by the notice. RCW 19.255.010(2)-(3). The Notice of Phishing Incident does not mention the involvement of law enforcement.

6.10 In its Notice of Phishing Incident, Overlake claims that it began to notify affected patients out of an "abundance of caution." See Exhibit 1. However, RCW 19.255.010(1), Washington's Data Breach Notification law, required Defendants to issue the notice "if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and the personal information was not secured." RCW 19.255.010(1). The same statute gives a specific exemption from the notice requirement "if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm." *Id.*

[4] *Id.*

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

6.11 Defendants did not just send out notice "in an abundance of caution," but also because they "reasonably believed" that the personal information of Plaintiff and Class Members "were acquired by an unauthorized person," that the "personal information was not secured," and because it was "reasonably likely to subject consumers to a risk of harm."

6.12 Even worse, further demonstrating their apparent lack of concern for consumers, it does not appear Defendants have even offered persons affected by the Data Breach complimentary credit monitoring and/or identity protection services.

6.13 Overlake had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

6.14 Plaintiff and Class Members provided their Private Information to Overlake with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

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

6.16 Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and ***hospitals*** are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[5]

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

---

[5] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (emphasis added).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

6.18 Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Overlake's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

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

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

workforces in violation of 45 C.F.R. § 164.306(a)(4);

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

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption").

6.19 As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Overlake negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

6.20 Accordingly, as outlined below, Plaintiff's and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiff and the Class Members also lost the benefit of the bargain they made with Overlake.

VII. CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

7.2 Cyberattacks and data breaches at medical facilities like Overlake are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

7.3 Researchers have found that at medical facilities that experienced a data security

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

incident, the death rate among patients increased in the months and years after the attack.[6]

7.4 Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[7]

7.5 Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.[8]

7.6 The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

7.7 The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

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

7.9 Identity thieves can also use Social Security numbers to obtain a driver's license or

---

[6] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks

[7] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

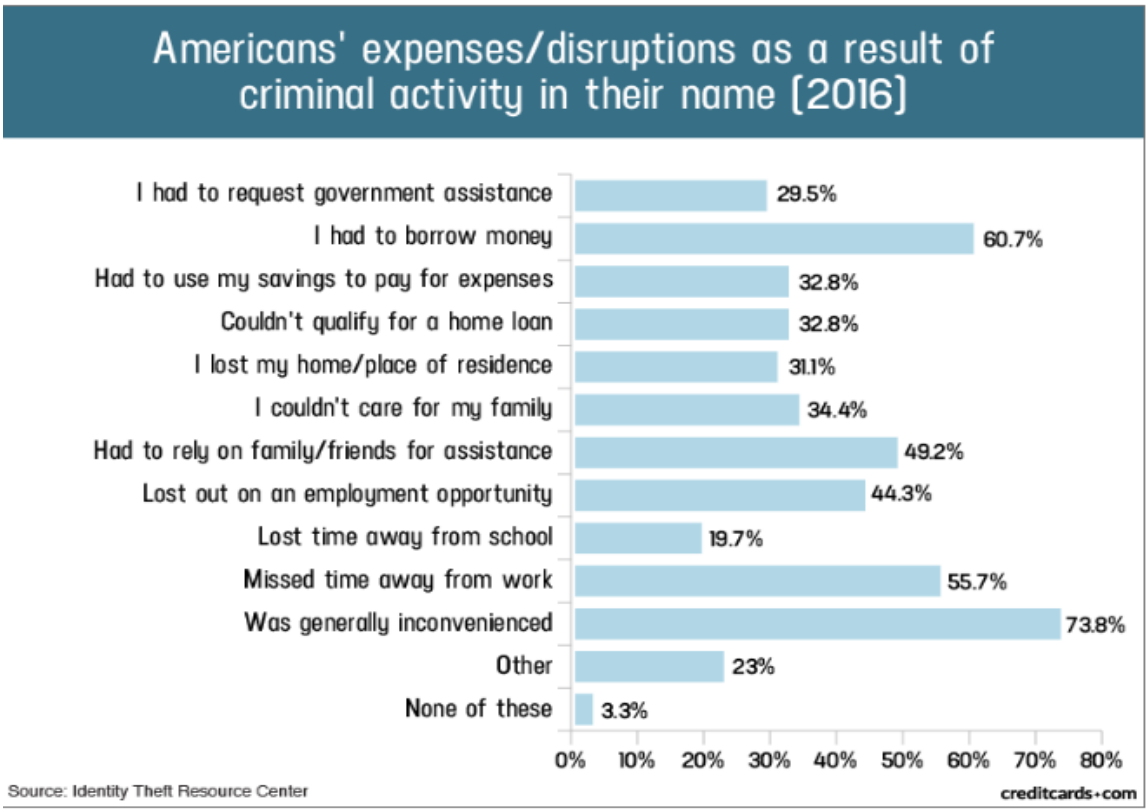
[8] *Id.*

[9] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[10] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[11]



7.10 Moreover, theft of Private Information is also gravely serious. PII/PHI is a valuable

[11] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

property right.[12] Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

7.11 Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[13] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

7.12 It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

---

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

[13] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 18, 2020).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

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

7.14 There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

7.15 Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[14]

7.16 Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendants therefore knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VIII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

8.1 To date, Defendants have done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

8.2 Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

8.3 Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

[14] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

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

8.5 As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

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

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

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

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

8.10 Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of Overlake's computer property and protect Plaintiff's and Class Members' Private Information. Upon information and belief, Defendants entirely fund their data security systems and operations from revenue derived from patients, have no independent dedicated source of funding for data security,

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

and thereby agree to use part of the price paid by Plaintiff and Class Members (or entities paying on their behalf) to provide adequate data security. Thus, Plaintiff and the Class Members did not get what they paid for.

8.11 Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

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

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

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. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

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

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

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

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

8.14 Further, as a result of Overlake's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

8.15 As a direct and proximate result of Overlake's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

IX. CLASS ACTION ALLEGATIONS

9.1 Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

9.2 Plaintiff proposes the following Class definition, subject to amendment as appropriate:

9.3 All individuals whose Private Information was received, gatherer, shared, obtained, or otherwise found itself in the possession of Defendants and compromised in the Data Breach.

9.4 Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

9.5 Numerosity. CR 23(a)(1). The members of the Class are so numerous that joinder

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class may approach 109,000 patients.

9.6 Commonality. CR 23(a)(2) & (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

9.7 Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

9.8 Whether Defendants knowingly concealed notification to affected customers of the Data Breach

9.9 Whether Defendants unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

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

9.11 Whether Defendants' conduct was negligent;

9.12 Whether Defendants violated the requirements of the Washington State Healthcare Information Act, RCW 70.02.005 et seq.;

9.13 Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

9.14 Whether Defendants' acts, inactions, and practices complained of herein violated Plaintiff and Class Members' Washington Constitutional Right to Privacy;

9.15 Whether Defendants' acts, inactions, and practices complained of herein violated the Washington State Consumer Protection Act; and

9.16 Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

9.17 Typicality. CR 23(a)(3). Plaintiff's claims are typical of those of other Class

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

members because Plaintiff's information, like that of every other Class member, was misused, and/or disclosed by Defendants.

9.18 Adequacy of Representation. CR 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

9.19 Superiority of Class Action. CR 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class Members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

9.20 Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

9.21 Defendants have acted or refused to act on grounds that apply generally to the Class, as alleged above, and certification is proper under CR 23(b)(2).

CAUSES OF ACTION

X. FIRST COUNT

Violation of the Washington State Uniform Healthcare Information Act (RCW 70.02.005 *et seq.*)

(On Behalf of Plaintiff and All Class Members)

10.1 Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein. Section 70.02.02 of the Revised Code of Washington provides that "Except as authorized elsewhere in this chapter, a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

other person without the patient's written authorization. A disclosure made under a patient's written authorization must conform to the authorization."

10.2 At all relevant times, Defendants were health care providers because they were authorized by the laws of Washington State to provide health care in the ordinary course of their business or practice. RCW 70.02.010(19).

10.3 At all relevant times, Defendants collected, stored, managed, and transmitted Plaintiff and Class Members' PII/PHI.

10.4 Plaintiff and Class Members PII/PHI is "Health Care Information" under RCW 70.02.010(17) in that it identifies or can be readily associated with the identify of a patient and directly relates to the patient's health care or that it is a required accounting of disclosures of health care information.

10.5 The Revised Code of Washington requires Defendants to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to them and maintained by them. Specifically, RCW 70.20.020 prohibits Defendants from disclosing Plaintiff and Class Members' PHI without first obtaining their authorization to do so.

10.6 RCW 70.20.020-030 specifies the manner in which authorization must be obtained before PHI is released. Defendants, however, failed to obtain any authorization—let alone, proper authorization—from Plaintiff and Class Members before releasing and disclosing their PHI. As mandatorily required by RCW 70.20.150 (Security safeguards), Defendants also failed to effect reasonable safeguards for the security of all health care information they maintain, including but not limited to failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PHI. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff and Class Members' PHI was disclosed. By disclosing Plaintiff and Class Members' PHI without their written authorization. Defendants violated RCW 70.20.10 et seq., and their legal duty to protect the

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

confidentiality of such information.

10.7 As a direct and proximate result of Overlake's' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violation of the RCW 70.20, pursuant to RCW 70.20.170, Plaintiff and Class Members also are entitled to (1) injunctive relief; (2) actual damages per Plaintiff and each Class member, and; (3) reasonable attorneys' fees and all other expenses.

XI. SECOND COUNT

Violation of the Washington State Consumer Protection Act (RCW 19.86.010 *et seq*.)

(On Behalf of Plaintiff and All Class Members)

11.1 Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

11.2 The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

11.3 Defendants are "persons" as described in RWC 19.86.010(1).

11.4 Defendants engage in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

11.5 By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendants' practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

11.6 In the course of conducting their business, Defendants committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement,

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PII/PHI, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

11.7 Defendants also violated the CPA by failing to timely notify and concealing from Plaintiff and Class Members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

11.8 Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendants' wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

11.9 The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

11.10 As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII/PHI; (5) deprivation of the value of his or her PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

11.11 Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

11.12 Plaintiff, on behalf of herself and the Class Members also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of herself and the Class Members requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

XII. THIRD COUNT

Negligence

(On Behalf of Plaintiff and All Class Members)

12.1 Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

12.2 Plaintiff brings this claim individually and on behalf of the Class members.

12.3 Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen,

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

misused, and/or disclosed to unauthorized parties.

12.4 Defendants had, and continue to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

12.5 Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

12.6 Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPPA and Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

12.7 Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

12.8 Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

12.10 Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

12.11 Defendants systematically failed to provide adequate security for data in their possession.

12.12 The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards.

9.22 Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendants' possession.

9.23 Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

9.24 Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendants' possession might have been compromised and precisely the type of information compromised.

9.25 It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

frequency of cyberattacks and data breaches in the medical industry.

9.26 It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

9.27 Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

9.28 As a result of Defendants' ongoing failure to notify Plaintiff and Class Members regarding what type of Private Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

9.29 Defendants' breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

9.30 As a result of Defendants' negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

9.31 Plaintiff seeks the award of actual damages on behalf of the Class.

9.32 In failing to secure Plaintiff's and Class Members' Private Information and promptly notifying them of the Data Breach, Defendants are guilty of oppression, fraud, or malice, in that Defendants acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of herself and the Class.

9.33 Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendants to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendants to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

XIII. FOURTH COUNT

Breach of Express Contract

(On Behalf of Plaintiff and All Class Members)

15.1 The preceding factual statements and allegations are incorporated by reference.

15.2 Plaintiff and Class Members entered into express contracts with Defendants that include Defendants' promise to protect nonpublic personal information given to Defendants or that Defendants gather on their own from disclosure. The express contract is embodied in the Privacy Notice.

15.3 Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and gave Defendants their Private Information.

15.4 Defendants should have used some of Plaintiff's payments (or payments made on her behalf) to institute adequate protection of Plaintiff's Private Information, but Defendants did not.

15.5 As a result, Defendants exposed Plaintiff's Private Information during the Data Breach.

15.6 Plaintiff and Class Members thus paid Defendants for promised data security protections that they never received.

15.7 Had Plaintiff known of Defendants' substandard methods of protecting her Private Information, she would have sought medical care elsewhere.

15.8 Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was accessed by unauthorized personnel as part of the Data Breach.

15.9 As a direct and proximate result of the breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

XIV. FIFTH COUNT

Breach of Implied Contract

(On Behalf of Plaintiff and All Class Members)

16.1 The preceding factual statements and allegations are incorporated by reference.

16.2 Defendants provided Plaintiff and Class Members with an implied contract to protect and keep Defendants' patients' private, nonpublic personal, financial and health information when they gathered the information from each of their patients.

16.3 When Plaintiff and Class Members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

16.4 Defendants' agreement to reasonably protect such information included compliance with healthcare industry data security standards, and with applicable data security standards that govern healthcare entities like Defendants, including HIPAA.

16.5 Defendants solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

16.6 In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

16.7 HIPAA requires covered entities like Defendants to protect against reasonably anticipated threats to the security of sensitive patient health information.

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

16.9 Healthcare industry standards for data security include several best practices that have been identified that a minimum should be implemented by healthcare providers like

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Defendants. These include, but are not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

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

16.11 Class Members who paid money to Defendants, or who had money paid on their behalf to Defendants, reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security that complied with healthcare industry data security standards and applicable regulations like HIPAA. Defendant failed to do so.

16.12 Plaintiff and Class Members would not have provided their personal, financial or health information to Defendants, but for Defendants' implied promises to safeguard and protect Defendants' patients' private personal, financial, and health information.

16.13 Plaintiff and Class Members performed their obligations under the implied contract when they provided their private personal, financial, and health information as a patient and when they paid for the services provided by Defendants.

16.14 Defendants breached the implied contracts with Plaintiff and Class Members by failing to protect and keep private the nonpublic personal, financial, and health information provided to them about Plaintiff and Class Members.

16.15 As a direct and proximate result of Defendants' breach of their implied contracts, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

XV. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. Ordering Defendants to disseminate individualized notice of the Data Breach to all Class Members;

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

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

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

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

K. Such other and further relief as this court may deem just and proper.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

RESPECTFULLY SUBMITTED this 16th day of July 2020.

FRANK FREED SUBIT & THOMAS LLP

By: */s/ Michael C. Subit*

Michael C. Subit, WSBA No. 29189
705 Second Avenue, Suite 1200
Seattle, Washington 98104-1798
(206) 682-6711 (phone)
(206) 682-0401 (fax)
msubit@frankfreed.com

MASON LIETZ & KLINGER LLP

By: */s/ David K. Lietz*

David K. Lietz (DC Bar No. 430557)
Admitted Pro Hac Vice
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
dlietz@masonllp.com

Attorneys for Plaintiff and the Proposed Classes

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was served via King County E-Service and/or email upon the following:

Paul Karlsgodt, WSBA No. 40311
BAKER & HOSTETLER, LLP
1801 California St Ste 4400
Denver, CO 80202-2662
Tel: 303.764.4013
E-mail: pkarlsgodt@bakerlaw.com

James R. Morrison, WSBA No. 43043
James Barnao, WSBA No. 56221
BAKER & HOSTETLER, LLP
999 Third Avenue, Suite 3600
Seattle, WA 98104 Tel: 206.332.1380
E-mail: jmorrison@bakerlaw.com
jbarnao@bakerlaw.com

Attorneys for Defendants

DATED this 16th day of July 2020.

/s/ Sarah Gunderson
Sarah Gunderson

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711