UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

YVONNE MART FOX, GRANT NESHEIM, DANIELLE DUCKLEY, and SHELLEY KITSIS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

IOWA HEALTH SYSTEM, doing business as UNITYPOINT HEALTH, an Iowa non-profit corporation,

Defendant.

Case No.: 18-cv-327

SECOND AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs YVONNE MART FOX ("Fox"), GRANT NESHEIM ("Nesheim"), DANIELLE DUCKLEY ("Duckley"), and SHELLEY KITSIS ("Kitsis") (Fox, Nesheim, Duckley, and Kitsis may be individually and collectively referred to herein as a "Plaintiff" or "Plaintiffs"), individually and on behalf of all other persons similarly situated, by their undersigned attorney, file this Second Amended Class Action Complaint against IOWA HEALTH SYSTEM, doing business as UnityPoint Health ("UnityPoint" or "Defendant") to, without limitation, obtain actual and exemplary damages, injunctive relief, restitution, and obtain a declaration that Defendant's actions were unlawful as further set forth below. Plaintiffs allege the following based upon personal knowledge as to themselves and their own acts, and on information and belief as to all other matters, including, *inter alia*, any investigation conducted by and through their attorney.

NATURE OF THE ACTION

1. Defendant UnityPoint is a multi-hospital delivery and health care system serving parts of Wisconsin, Iowa, and Illinois. UnityPoint's patient data, including the protected health information belonging to Plaintiffs, was breached and stolen, or as UnityPoint charitably puts it, "compromised", from as far back as November 1, 2017 (the "First Data Breach"). UnityPoint reportedly discovered the data breach between February 7, 2018 and February 15, 2018.

2. On or about April 17, 2018 Plaintiffs Fox and Nesheim received a form letter notifying them that the data breach "may have resulted in unauthorized access to some protected health information." In other words, Plaintiffs' electronic medical records were stolen. The letter informed Plaintiffs that UnityPoint wanted to make Plaintiffs aware of the situation and suggested certain practices "as a general matter" that individuals can follow to help protect themselves against medical identity theft. The notification letter did not mention whether Defendant would take any steps to remediate the harm from the data breach, including whether it would offer protective services such as credit monitoring, identity theft protection, or "dark web" searches.

3. Then, UnityPoint's patient data, including protected health information belonging to Plaintiffs, was again breached and stolen, or as UnityPoint once again charitably puts it, "compromised", from as far back as March 14, 2018 (the "Second Data Breach"). UnityPoint reportedly discovered the data breach May 31, 2018. Individually and collectively the First Data Breach and Second Data Breach are referred to herein as the "Data Breach" or "Data Breaches".

4. On or about August 2, 2018, Plaintiffs received a form letter notifying them that the Second Data Breach "may have resulted in unauthorized access to some protected health information and other personal information for some patients. Our investigation indicates that some of your information was contained in one or more of the compromised email accounts." In

other words, just as in the First Data Breach, Plaintiffs' electronic medical records were stolen.

5. The letter informed Plaintiffs that UnityPoint wanted to make Plaintiffs aware of the Second Data Breach and what the victims could do to protect themselves against medical identity theft by "monitoring [their] health information." The notification letter further stated,

> "To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft." [**Emphasis in original**.]

6. The letter neglected to mention that in addition to being a credit bureau, Experian is also a data broker, and that in or around October 2015 Experian harmed millions of consumers when it failed to protect their personal information from being exposed to identity thieves on the dark web. Consumers' social security numbers and credit card security codes were among the data compromised during the Experian breach, which began in 2015 and lasted over an 18-month period. Experian then broke the law by not telling these consumers the truth about what happened. In the Experian data breach hackers obtained $65 million from fraudulent tax returns as a result of the breach.

7. Plaintiffs, and the patients and consumers they seek to represent, are victims of Defendant's negligence and unfair practices who have suffered tangible and concrete injury-in-fact. Accordingly, Plaintiffs, on their own behalves and on behalf of a class of similarly situated individuals (the "Class" or "Class Members" as further defined below), bring this lawsuit and seek injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in the possession of Defendant.

JURISDICTION AND VENUE

8. This Court has original jurisdiction pursuant to the Class Action Fairness Act,

28 U.S.C. § 1332(d) because: (a) at least one member of the putative Class is a citizen of a state different from UnityPoint; (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs; (c) the proposed Class consists of more than 100 Class Members; and (d) none of the exceptions under the subsection apply to this action.

9. Pursuant to 28 U.S.C. § 1367 this Court has supplemental jurisdiction over the state statutory and common law claims alleged herein.

10. This Court has personal jurisdiction over Defendant because: (a) it is registered to, and in fact does, conduct business in Wisconsin; and (b) has sufficient minimum contacts in Wisconsin, or otherwise intentionally avails itself of the markets within Wisconsin through the promotion, sale, marketing, and distribution of its services, to render the exercise of jurisdiction by this Court proper and necessary.

11. Venue is proper in this District under 28 U.S.C. § 1391 because: (a) Plaintiffs Fox and Nesheim are residents of, and domiciled in, this District; (b) Defendant conducts substantial business in this District; and (c) a substantial part of the events giving rise to Plaintiffs' claims alleged herein occurred in this District.

PARTIES

12. Plaintiff Yvonne Mart Fox is a natural person and citizen of the state of Wisconsin, residing in Middleton, Wisconsin.

13. Plaintiff Grant Nesheim is a natural person and citizen of the state of Wisconsin, residing in Mazomanie, Wisconsin.

14. Plaintiff Danielle Duckley is a natural person and citizen of the state of Illinois residing in Silvis, Illinois.

15. Plaintiff Shelley Kitsis a natural person and citizen of the state of Iowa residing in Des Moines, Iowa.

16. Defendant Iowa Health System is a non-profit corporation organized and existing under the laws of the State of Iowa with its principal place of business located 1776 West Lakes Parkway, Suite 400, West Des Moines, Iowa 50266. Defendant transacts business throughout Dane County, the state of Wisconsin, and the states of Iowa and Illinois. Defendant does business as UnityPoint Health. At all times material to this action, acting alone or in concert with others, UnityPoint has advertised, marketed, distributed, and sold its health care services to patients and consumers in the state of Wisconsin and in the states of Iowa and Illinois.

COMMON FACTUAL ALLEGATIONS

17. Defendant UnityPoint (known as Iowa Health System until 2013) is a network of hospitals, clinics, home care services, and health insurers in Wisconsin, Iowa, and Illinois. Defendant's health system now encompasses eight metropolitan areas in three states.

18. At least as early as the period between February 7, 2018 and February 15, 2018, UnityPoint discovered that at least 16,429 patients' and consumers' personal and protected health information, including patient names, birth dates, diagnosis codes, addresses, private mobile and landline phone numbers, email addresses, medical record numbers, treatment information, diagnoses, lab results, medications, providers, dates of service, insurance information, policy numbers, Medicare numbers, billing information, other financial information, and Social Security numbers (the "Personal Health Information" or "PHI"), had been accessed through one or more employees' email account(s) in connection with the First Data Breach.

19. Then, on or about May 31, 2018, UnityPoint discovered that 1.4 million patients' and consumers' PHI and other personal information, had again been accessed through one or more

employees' email account(s) in connection with the Second Data Breach. The Second Data Breach disclosed and exposed PHI that was accessed and stolen from as far back as March 14, 2018. Defendant claims the Second Data Breach went undetected for several months. Upon discovery, rather than immediately disclose the Second Data Breach and inform patients, the public, and regulators of what occurred, UnityPoint waited two months before it acknowledged PHI had been stolen.

The First Data Breach and First Notice Letter

20. UnityPoint ultimately admitted the First Data Breach to its patients, consumers, and the public on or about April 16, 2018. In a notification form letter from RaeAnn Isaacson, Privacy Officer for UnityPoint to Plaintiffs and Class Members dated April 16, 2018 (the "First Notice Letter" or "First Letter"), UnityPoint admitted it had,

> "discovered your protected health information was contained in an impacted email account, including your name and one or more of the following: date of birth, medical record number, treatment information, surgical diagnosis, lab results, medication(s), provider(s), date(s) of service and/or insurance information."

21. In an effort to minimize the harm, UnityPoint did not disclose all the true facts about the First Data Breach in the First Notice Letter when it falsely claimed, “The information did not include your Social Security number."

22. The First Notice Letter further admitted that, "[w]e want to make impacted individuals aware of the situation so they can take precautionary measures to protect their health information.” The First Notice Letter then further falsely claimed UnityPoint had no information indicating that the stolen PHI "will be used for any unintended purposes." Defendant's Letter then listed some practices "[a]s a general matter" that individuals can take to protect themselves from medical identity theft, including:

- "Only share your health insurance cards with your health care providers and

other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize."

23. The First Notice Letter did not mention whether Defendant would take any steps to remediate the First Data Breach, or whether it would offer protective services such as credit monitoring and identity theft protection. The First Notice Letter did not mention whether Defendant had notified law enforcement or the Federal Trade Commission of the First Data Breach. The First Notice Letter neither referred victims to any website for assistance (such as the Federal Trade Commission's identity theft website), nor suggested Plaintiffs and the Class Members consider any of the following precautions: notifying local law enforcement (except for Iowa residents); getting a free copy of their credit report; monitoring their credit for signs of identity theft; placing a fraud alert on their credit report; requesting a credit freeze; notifying their insurance companies, health providers, and financial institutions; requesting their insurance companies, health providers, and financial institutions notify them of possible instances of identity theft; requesting new account numbers; or closing accounts. The First Notice Letter did not describe any steps Defendant is taking to investigate the First Data Breach, protect against future breaches, or remediate or mitigate the harm from the First Data Breach such as searching for and locating the stolen PHI.

24. Unbeknownst to Plaintiffs at the time, on or about April 16, 2018 UnityPoint

admitted to the Wisconsin Department of Agriculture, Trade and Consumer Protection (the "DATCP Filing") that the data stolen did in fact include "Social Security numbers, dates of birth, medical record numbers, treatment & surgical information, insurance, and other financial information." This is the type and, at a minimum, the scope of sensitive PHI data and particular information the cyber-criminals were motivated to steal, which they desired, which they were after, which they specifically targeted, and which Defendant admits they accessed and stole in the Data Breach.[1]

25. Nowhere did Defendant describe any steps it is taking to protect against future breaches, or remediate and mitigate the harm from the First Data Breach. Instead of notifying Plaintiffs and the Class Members of the actual steps Defendant is taking to prevent data breaches and mitigate the existing harm, Defendant only proclaimed in the DTCPA Filing that,

> "Upon learning of the incident, UnityPoint Health promptly took action to secure the impacted email accounts, changed passwords, and engaged external cybersecurity professionals to analyze what information might have been contained in the impacted accounts."

Rather than informing Plaintiffs and the Class Members what it is going to do about the stolen PHI, UnityPoint only offers up a "sincere apology", essentially telling the First Data Breach victims, "you're on your own" ("YOYO").

[1] To date, Defendant has failed to provide Plaintiff Fox and other Class Members with a true and complete accounting or copies of her PHI that was stolen despite several requests. In addition, while Defendant claims it has engaged external cybersecurity professionals to analyze the Data Breach, it has not disclosed the results of such analysis. If anyone can point to markers identifying the cyber-criminals (*i.e.*, through "dark web" searches, tracing TOR traffic, network surveillance, or analyzing TOR bridge, relays, mirror directories, node destination IP addresses, and exit nodes) it is Defendant who can and should do so rather than attacking Plaintiff Fox for her inability to identify the thieves.

26. However, while Plaintiffs Fox and Nesheim and the other Class Members who were victimized by the First Data Breach were and are being given the YOYO response, and are being told that there would be no remedial action from UnityPoint and no assistance or monetary compensation, the truth is Defendant recognized that actual harm and injury is being, and will continue to be, caused directly by the First Data Breach, and *had* purchased some form of limited credit monitoring services for up to a year for some Class Members affiliated with Defendant. The select UnityPoint affiliates have suffered the same injury and harm as the Plaintiffs and Class Members that is directly traceable to the same First Data Breach.[2]

27. Plaintiffs and other Class Members have suffered injury[3] that can be directly traceable to Defendant from the misuse of the stolen PHI and other personal information acquired in the First Data Breach without authorization, including without limitation the following:

a. one Class Member received a call from a UnityPoint employee in Iowa telling her that her PHI "went out and was on 5 reports . . . [and] even the last visit with [her] primary physician was included";

b. another Class Member has received a marked and unmistakable increase since the First Data Breach in illegal robo-dialed calls on her mobile and home telephones as well as spam emails linked to the Data Breach, including 27 unrecognized robo-dialed calls on her home telephone number during the period from April 6, 2018 to May 10, 2018;

---

[2] While this action may or may not not be admissible as proof of negligence, or culpable conduct, it shows that Defendant admits the Class Members' injury is actual, imminent, and feasible to monitor.

[3] "Injury" is defined by Black's Online Law Dictionary as "*Any wrong* or damage *done to another*, either *In his* person, *rights*, reputation, or property. *Parker v. Griswold*, 17 Conn. 298, 42 Am. Dec. 739; *Woodruff v. Mining Co.*, 18 Fed. 781; *Hitch v. Edgecombe County*, 132 N. C. 573, 44 S. E. 30; *Macauley v. Tierney*, 19 R. I. 255, 33 Atl. 1, 37 L. R. A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of any one, whereby his body, *his dignity*, or his reputation is maliciously injured. Voet, Com. ad Pand. 47, t. 10, no. 1." Black's Law Dictionary, Online, 2nd Ed. [*Emphasis added*.]

c. another Class Member reports that since the First Data Breach he has been trying to get more support from Unity and has failed to even get help with credit protection, "plus the number of scam medical calls is rising";

d. another Class Member who was hospitalized multiple times since February 2016 reports that she is "horrified" and is "experiencing extreme anxiety" and other personal health issues "due to the release of [her] private information" about her medical treatment;

e. another Class Member has received a marked and unmistakable increase since the First Data Breach in unauthorized login attempts in connection with her online accounts, including email, financial, e-commerce, and other internet account sites, and as a result has had to change her "passwords, debit cards. Any thing (sic) private"[4]; and

f. another Class Member who inquired about the status of her PHI was falsely and repeatedly told "that no social security numbers have been involved, that no HIPPA violation occurred".

28. Plaintiffs Fox and Nesheim each received a copy in the mail of the First Notice Letter on or about April 17, 2018. The Notice Letter did not state how many persons had their PHI stolen, the actual size and complete scope of the First Data Breach, whether Defendant would pay to or otherwise take precautionary measures to address, remediate, and mitigate its patients' injury, or whether Defendant would offer protective services such as credit and identity theft protection.

[4] Unfortunately, hackers often copy these types of "suspicious sign in prevented" emails to steal other people's account information. As a result of the Data Breach, Plaintiffs and the Class Members are now at a heightened risk of being further victimized by these types of "phishing emails" and must be extra wary of messages that ask for personal information like usernames, passwords, or other identification information, or send them to unfamiliar websites asking for this information. Heads the cyber-criminals win by further victimizing Plaintiffs and the Class Members from inundating them with "phishing emails", tails Plaintiffs and the Class Members lose by being subjected to actual unauthorized sign in attempts to steal the information in their accounts. Either way, Plaintiffs and the Class Members are being injured and harmed.

29. The First Data Breach is not the first evidence of UnityPoint's failure to secure PHI during the last 24 months. On May 11, 2016, a UnityPoint Health Affiliated Covered Entity healthcare provider in Iowa notified the U.S. Dept. of Health and Human Services Office for Civil Rights (the "HHS") of an unauthorized access/disclosure of electronic medical records affecting 1,620 individuals. Additionally, UnityPoint affiliated healthcare provider UW Health notified the HHS on May 25, 2017 of an email hacking/IT incident affecting 2,036 individuals.[5]

30. Rather than taking steps to fairly and fully inform Plaintiffs and the Class Members about the true facts regarding the First Data Breach and take its own "precautionary measures" to mitigate and remediate at its cost the injury to affected patients, Defendant instead misrepresented the nature, breadth, scope, harm, and cost of the First Data Breach to Plaintiffs and the Class Members when it falsely stated in the Notice Letter that, "The [stolen] information did not include your Social Security number", and "[w]e have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes."

31. Social Security numbers are wrapped up in most aspects of Americans' lives—employment, medical history, taxes, education, bank accounts, and so on. Criminals who get their hands on stolen Social Security numbers can create numerous crimes, including without limitation, opening financial accounts, getting medical care, prescriptions, and equipment, poaching health insurance coverage (tainted or falsified medical data, such as listing the wrong blood type, can have deadly consequences), filing for false or fraudulent tax refunds (in 2016, the IRS identified $227 million lost in fraudulent tax returns), and to steal Social Security benefits themselves.

[5] UnityPoint and UW Health received regulatory approval from the Federal Trade Commission approval for their joint operating agreement on or about April 11, 2017.

32. Defendant knew, or should have known, when it sent the Notice Letter that the stolen information did include affected patient Social Security numbers.[6] Defendant further knew, or should have known, it possessed information that makes it highly likely the PHI will be used for an unintended purpose. Defendant knowingly, intentionally, and recklessly made these false statements in an effort to conceal and minimize the harm and injury to Plaintiffs and the Class Members caused by the First Data Breach, and to induce them and the public to continue to use, and to expand the use of, Defendant's services.

The Second Data Breach and Second Notice Letter

33. UnityPoint ultimately admitted the Second Data Breach to its patients, consumers, and the public on or about July 30, 2018. In a notification form letter to Plaintiffs and Class Members, again signed by RaeAnn Isaacson, Privacy Officer for UnityPoint dated July 30, 2018 (the "Second Notice Letter" or "Second Letter"), UnityPoint admitted "compromised" email account(s) were accessed that,

> " included your name and one or more of the following information: address, date of birth, Social Security number, driver's license number, medical record number, medical information, treatment information, surgical information, diagnosis, lab results, medication(s), provider(s), date(s) of service and/or insurance information."

34. In an effort to minimize the harm, Defendant falsely claimed that its "electronic medical " systems were not impacted by the Second Data Breach because the stolen PHI was "contained in the body an email or in attachments such as reports." Apparently in Defendant's world, transmitting PHI to "support patient care" through its insecure electronic business email

[6] Insurance information, which UnityPoint admits was stolen, includes Medicare claim numbers which are the Social Security number of the primary wage earner on which benefits are based, plus an appropriate letter code.

system is not part of its "electronic medical record system[s]".

35. Plaintiffs and other Class Members have suffered injury[7] that can be directly traceable to Defendant from the misuse of the stolen PHI and other personal information acquired in the Second Data Breach without authorization, including without limitation experiencing a marked and unmistakable increase since the Second Data Breach in spam emails and illegal robo-dialed calls on their mobile and home telephones, resulting in having to change phone numbers; unauthorized login attempts in connection with online accounts (including email, financial, e-commerce, and other internet account sites) resulting in having to change passwords and/or cancel accounts; and having personal identifiers disclosed on the dark web, all linked to the Data Breach.

36. Because of identity theft and fraud directly linked to the Second Data Breach, one Class Member has had to replace three of her credit cards, change her email address, change her phone number, and take 20 hours off of work to try and repair the harm and injury done to her that is directly traceable to the Second Data Breach. To make matters even worse, she received a Second Notice Letter about the Data Breach regarding the theft of her deceased father's PHI which she will now have to deal with as well.

PHI is Stolen for Misuse and Defendant's Purchase of Protection Proves the Risk

37. The gravamen of this lawsuit is that Defendant failed to keep Plaintiffs' and the Class Members' PHI confidential, whether knowingly and willfully or negligently, as required by

[7] "Injury" is defined by Black's Online Law Dictionary as "*Any wrong* or damage *done to another*, either *In his* person, *rights*, reputation, or property. *Parker v. Griswold*, 17 Conn. 298, 42 Am. Dec. 739; *Woodruff v. Mining Co.*, 18 Fed. 781; *Hitch v. Edgecombe County*, 132 N. C. 573, 44 S. E. 30; *Macauley v. Tierney*, 19 R. I. 255, 33 Atl. 1, 37 L. R. A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of any one, whereby his body, *his dignity*, or his reputation is maliciously injured. Voet, Com. ad Pand. 47, t. 10, no. 1." Black's Law Dictionary, Online, 2nd Ed. [*Emphasis added*.]

law, and that Plaintiffs and the Class Members have suffered legally cognizable concrete and tangible injury as a result. Plaintiffs' and the Class Members' stolen PHI is being misused by cyber-criminals right now, today, and that misuse is ongoing, without authorization, and is directly and fairly traceable to the Data Breach

38. State legislatures have identified the harm from unauthorized disclosure of PHI as sufficient to permit suit.[8] As one statutory example, the Wisconsin legislature is so serious about protecting the confidentiality of PHI, it chose, without limitation, to subject anyone who negligently discloses such information to a forfeiture of up to $1,000 per violation, and to subject those who intentionally and knowingly disclose such information for pecuniary gain to imprisonment for not more than 3 years and 6 months. Wis. Stat. § 146.84(2)(b) and (c).

39. Just as common law permits suit in instances such as for slander *per se* or trespass where *damages* (damages are distinct from injury or harm) may be difficult to quantify or prove, the violation of Plaintiffs' and the Class Members' right to confidentiality of their PHI granted by law, including under Wis. Stat. §§ 146.82 and 146.84, is sufficient to constitute actionable injury-in-fact. Plaintiffs and the Class Members injury is actual *de facto* injury from the invasion of a legally protected interest, regardless of whether the nature of that injury is coupled with monetary damages from identity theft, internet account hacking, financial fraud, or out of pocket cost to mitigate the actual, ongoing, imminent, and immediate harm from the Data Breach on the one hand, or from illegal telephone calls and emails, harassment, embarrassment, an affront to one's dignity, or personal injury on the other. In this case, not only is the injury from a violation of

[8] "Any person [] who negligently violates s. 146.82 or 146.83 shall be liable to any person injured as a result of the violation . . ." Wis. Stat. § 146.84(1)(b) and (bm). "An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection.

Defendant's confidentiality obligation legally cognizable, but also the *de facto* injury from the invasion and wrong committed against the legally protected interests of the Plaintiffs and the Class Members actually exists, is concrete and particularized, is tangible, and is ongoing. It is not merely conjectural or hypothetical. *See, e.g.*, Wis. Stat. §§ 146.82 and 146.84.

40. The act of stealing or improperly accessing Plaintiffs' and the Class Members' PHI, and the cyber-criminals' purpose in stealing Plaintiffs' and the Class Members' PHI, is to commit additional illegal acts and crimes, such as unlawful robo-dialed scam medical marketing campaigns targeted at Plaintiffs and the Class Members, gaining unauthorized access to their internet accounts, opening unauthorized financial accounts using the PHI, and both financial and medical identity theft to enter into unauthorized transactions using the PHI. Theft of data like the stolen PHI necessarily implies harm because the misuse of data is the only plausible explanation for the Data Breaches. Moreover, the fact that Defendant has purchased credit monitoring or identity theft protection services for affected customers supports this conclusion. UnityPoint would not have done so if the risk could be disregarded.

41. In addition to actual illegal robo-dialing campaigns and internet and financial identity theft suffered by Plaintiffs and the Class Members in this case, in a recent survey conducted by the Medical Identity Fraud Alliance (MIFA), a healthcare industry trade group, 52 percent of victims said their information was used to obtain government benefits like Medicare or Medicaid. And 59 percent had their identity used to obtain healthcare, while 56 percent said a scammer parlayed their data into prescription drugs or medical equipment. This is all the type of injury and harm, including actual fraud, Defendant knows full well has been reported to it as being suffered by Plaintiffs and the Class Members, and is directly traceable to the Data Breach. This harm is not merely just possible, not just certainly impending, it has actually happened and is

ongoing, and all Class Members are in imminent and immediate danger of being further subjected to this injury.

42. While Plaintiffs obviously can't be expected to read what's going on inside a cyber-criminal's mind, the fact is Defendant has received complaints about the known illegal use of the stolen PHI, including known instances of fraud, on Defendant's dedicated (and supposedly confidential) toll-free response lines which it established to answer victims' questions about the Data Breaches. The total number of reports involving the known illegal and fraudulent use of the stolen PHI is unknown to Plaintiffs, but Defendant knows the number and nature of these phone calls. For Defendant to claim that the purpose of the cyber-criminals' Data Breaches is unknown, or that it has not resulted in one known instance of fraud in the last eight months, is more than willfully ignorant (cyber-criminals don't steal PHI for fun); it is evidence of fraud, concealment, and a coverup.

Stolen PHI is Valuable

43. Stolen PHI is a one of the most valuable commodities on the criminal information black market. In 2014, the FBI warned healthcare organizations that PHI data is worth 10 times the amount of personal credit card data on the black market.[9] PHI data for sale is so valuable because PHI information is so broad, and it can therefore be used for a wide variety of criminal activity such as to create fake IDs, buy medical equipment and drugs that can be resold on the street, or combine patient numbers with false provider numbers to file fake claims with insurers.

[9] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. Dark web monitoring is a commercially available service which, at a minimum, Defendant can and should perform (or hire a third-party expert to perform).

44. The value of Plaintiffs' and the Class Members' PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" Internet websites, making the information publicly available, for a substantial fee of course.

45. It can take patients years to spot healthcare identity or PHI theft, giving criminals plenty of time to milk that information for as much cash as possible. That is precisely what makes medical data PHI more desirable to criminals than credit card theft. Credit card or financial information theft can be spotted by banks early on, and accounts can be quickly frozen or cancelled once the fraud is detected, making credit card and financial data much less valuable to criminals than PHI.

46. Defendant has disclosed and given access to the PHI of Plaintiffs and the Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant has opened up, disclosed, and exposed the PHI, email addresses, and telephone numbers of Plaintiffs and the Class Members to persons engaged in disruptive and unlawful business practices and tactics, including spam and "phishing" emails, robo-dialed calls, junk texts and faxes, other unwanted calls and communications, online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PHI.

47. In recognition of the value of PHI, today a growing number of legitimate companies are developing business models that center on giving consumers a choice on whether or not they themselves wish to monetize (*i.e.*, sell or rent) their "scrubbed" (*i.e.*, designed to be anonymous) health data. There are numerous startups that have built platforms to offer pay-to-access information to researchers from universities, medical institutes, and pharmaceutical companies—

and that allow consumers such as Plaintiffs and the Class Members to monetize their own PHI and turn a profit on it if they so choose.

48. Consumers who are customers of these startups receive compensation for allowing access to information such as that which was stolen in the Data Breaches, only anonymized or scrubbed.[10] By way of the Data Breaches, Defendant has compromised not only Plaintiffs' and Class Members' privacy, but also a substantial portion of the value of their PHI that is being misused and monetized by cyber-criminals.

49. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up to date technology security strategy, demonstrates a willful and conscious disregard for patient and consumer privacy, and has exposed the private information and PHI of Plaintiffs and 1.4 million other Class Members to unscrupulous operators, con artists, and outright criminals.

PLAINTIFF FOX'S EXPERIENCE

50. Plaintiff Yvonne Mart Fox is a resident of Middleton, Wisconsin. Ms. Fox has been a patient and user of UnityPoint and its affiliates' services since at least September 17, 2015. During the time Ms. Fox was a UnityPoint patient, she did not use the UnityPoint internet portal to see her PHI or to contact her physicians or their offices. Similarly, she did not communicate over the internet with UnityPoint or her physicians or their offices. In order to protect her privacy and minimize her digital footprint as much as possible, Ms. Fox chose to communicate with Defendant by phone or U.S. postal service mail.

[10] Users of startup CoverUS can potentially generate the equivalent of $100 to $1,000 a month if they choose to monetize their PHI depending on a user's health and demographics. Sicker people with special conditions that are of particular interest to researchers will likely be able to generate more money. Fast Company, "*Can This App That Lets You Sell Your Health Data Cut Your Health Costs*" by Ben Schiller, January 4, 2018.

51. In and around the period between December, 2017 and the end of February, 2017, Plaintiff Fox received an undated and unsigned letter from Defendant promising that, "[w]e will protect your medical records and privacy." However, unbeknownst to Ms. Fox, Defendant had already failed to protect her medical records and privacy, and commencing in and around the first quarter of 2018 Plaintiff began to notice an increase in the amount of unsolicited auto-dialed or robo-dialed phone calls, spam and phishing emails,[11] and unsolicited marketing and promotional communications on her mobile and landline telephones. Plaintiff Fox's mobile phone or data plan is limited, and unwanted junk texts or autodialed calls cause Plaintiff injury by restricting her available use.

52. During the period from April 13, 2018 to July 7, 2015, Ms. Fox received approximately 63 unwanted robo-dialed telephone calls on her land line. In particular, Ms. Fox has received a rash of the type of robo-dialed calls referred to by other Class Members as "scam medical calls", including calls from a number identified as "BC Health Clinics" on May 18, 2018 at 6:36 p.m., May 20, 2018 at 8:04 p.m., May 30, 2018 at 8:30 p.m. and 8:35 p.m., and June 9, 2018 at 9:39 p.m. Prior to the Data Breach, Ms. Fox experienced very few (*i.e.*, one or two), if any, robo-dialed calls per month, and none were of the scam medical type she is now experiencing.

[11] As recently as July 25, 2018 Plaintiff Fox received an email with a subject line "Critical security alert" stating, "Sign-in attempt was blocked". "Someone just used your password to try and sign into your account. [Name redacted] blocked them, but you should check what happened." This was followed by a suspicious looking link to "CHECK ACTIVITY". The email went on to say, "You received this email to let you know about important changes to your [Name redacted] Account and services." This is either an attempt to victimize Ms. Fox again by obtaining access to her online account with a "phishing email", or she is the victim of a cyber-criminal's unauthorized attempt to fraudulently gain access to her account. Either way, the increase Ms. Fox is experiencing since the Data Breach in this type of fraudulent activity is traceable to the Data Breach and is causing Ms. Fox injury and harm. *See also* footnote 6.

53. On or about April 17, 2018, Plaintiff Fox received a copy of the First Notice Letter in the mail signed by RaeAnn Isaacson, Privacy Officer for UnityPoint, containing the misrepresentations and omissions set forth herein, and admitting and confirming that her PHI in Defendant's possession had been stolen (obviously her PHI had been unlawfully viewed and accessed). Plaintiff then called UnityPoint on April 24, 2018 and spoke with a UnityPoint employee or representative named Ashley.

54. Plaintiff Fox inquired about the size and nature of the PHI, what specific PHI had been stolen in the First Data Breach, and what type of precautions UnityPoint was recommending and taking. In response, Ms. Ashley resorted to a scripted reply apologizing for the First Data Breach and repeating over and over the mantra that Plaintiff Fox "should take steps to protect her information."

55. Plaintiff told Ms. Ashley that she already did not use the internet to communicate with UnityPoint or review her records, and in response again received the same mantra from Ms. Ashley, namely "We are sorry, please take precautions to protect your information." Plaintiff Fox then asked if UnityPoint would pay for any precautions they were advising be taken in connection with the First Data Breach. Once again, Ms. Ashley repeated the exact same script: "We are sorry, please take precautions to protect your information."

56. Plaintiff then asked to speak to a supervisor, and Ms. Ashley said she would try to reach one. When Ms. Ashley came back on the line Plaintiff was told a supervisor would call her back in a few days.

57. Plaintiff told Ms. Ashley she did not want to wait "a few days" and was again met with the scripted words, "We are sorry, please take precautions to protect your information."

Frustrated in her efforts to obtain information by UnityPoint's stonewalling, Plaintiff Fox said goodbye to Ms. Ashley and hung up the phone

58. Within 15 minutes, Plaintiff Fox received a call from the number (503) 350-5979. The call was from someone purporting to be "Sujea" [sic] calling on Defendant's behalf. Once again, in response to Plaintiff's questions as set forth above, Ms. Sujea repeated the mantra: "We are sorry, please take precautions to protect your information."

59. Ms. Sujea repeated the mantra several times, only this time when Plaintiff asked if Defendant would pay for any appropriate precautions to mitigate the injury and harm from the First Data Breach, Plaintiff Fox was told there would be no further remedial action from UnityPoint and no assistance or monetary payments.

60. On or about August 2, 2018, Plaintiff Fox received a copy of the Second Notice Letter in the mail containing the misrepresentations and omissions set forth herein, and admitting and confirming that her PHI in Defendant's possession had been stolen in the Second Data Breach (obviously her PHI had been unlawfully viewed and accessed).

61. As a result of the Data Breaches, Plaintiff is being harassed and inundated with unwanted, unsolicited, and unlawful spam and phishing emails and auto-dialed calls from unscrupulous operators. These calls not only restrict Plaintiff's phone usage, but also use up amounts of Plaintiff's phone battery and the costs of the electricity needed to recharge her mobile phone. These spam emails and robo-dialed calls also cause Plaintiff annoyance, frustration, and wasted time. Plaintiff's privacy is being invaded as a direct result of the Data Breaches, and she and her property rights are being caused harm without her permission.

62. Aside from the financial loss consequences, both direct and indirect, that Plaintiff is facing, identity theft negatively impacts credit scores.[12] Because a criminal's delinquent payments, cash loans, or even foreclosures slowly manifest into weakened credit scores, and because this type of fraud takes the longest time to resolve, Plaintiff is therefore forced to subscribe to a credit monitoring service for the indefinite future.[13]

63. It can take years to spot healthcare identity or PHI theft, and Plaintiff has subscribed to an online credit monitoring service that provides online credit scores to consumers direct from the credit bureaus. This credit monitoring service does just what the name implies. It allows Plaintiff Fox to log in and see her credit report to determine if there is any suspicious activity such as a criminal trying to open an account in her name. But, it is nonetheless powerless to stop identity theft it in advance and does not indemnify her from, or insure her against, the harm caused by the Data Breaches.

64. Inexplicably, Defendant has failed to date to confirm the specific PHI of Plaintiff's that was stolen, and what other information in her medical records has been accessed without her consent, despite repeated requests to do so. This information is important for Plaintiff to know, especially given Defendant's YOYO response to the First Data Breach, its misrepresentations about the information (*i.e.*, no Social Security numbers) that was stolen, and the fact that the stolen PHI has in fact been misused so that she may make informed decisions regarding what further

[12] Direct financial loss refers to the amount of money stolen or misused by the identity theft offender. Indirect financial loss includes any outside costs associated with identity theft, like legal fees or overdraft charges. A 2014 Dept. of Justice study found that victims experienced a combined average loss of $1,343. In total, identity theft victims lost a whopping $15.4 billion in 2014.

[13] Defendant hypocritically refers to Plaintiffs Fox's subscription to a credit monitoring service as "manufacturing" damages while at the same time admitting the Class Members are suffering injury and harm by purchasing the same services for certain Class Members affiliated with Defendant.

action is appropriate to mitigate the injury and harm she is suffering, including purchasing or otherwise acquiring identify theft insurance. This unreasonable delay in dealing truthfully and in good faith with Ms. Fox means that she is in turn being unreasonably delayed in taking steps to protect herself (and in evaluating specifically which steps she should take) in addition to those that she has already taken (such as reporting it to law enforcement and regulators and applying for fraud alerts and a credit freeze) to mitigate the injury and harm caused her by the Data Breaches.[14]

65. All Plaintiff Fox knows for sure is that she has given UnityPoint every piece of information it has asked for during the course of her health care relationship with Defendant, including without limitation in oral communications with her physicians about her health, and in writing her address, phone number, date of birth, Medicare claim number, and gender as well as information on so-called intake forms describing the reasons she sought treatment.

66. As the amount of information from both unregulated sources that have identities and addresses attached (*i.e.*, phone books, search engines, and websites) and illegal sources (*i.e.*, stolen information like the PHI) grows over time, there is more and more information about who people might be. As a result, cyber-criminals are able to cross-references these two sources to marry unregulated data available elsewhere to criminally stolen data with an astonishingly

[14] Plaintiff Fox finds herself trying to "take precautions" against further injury and harm without knowing the specific information she needs which Defendant refuses to provide, although it admits there was a Data Breach. Defendant claims there is no injury or harm and that the First Data Breach is, in essence, no big deal. Apparently, in its world Defendant believes the consequences Ms. Fox is suffering from the First Data Breach and stolen PHI is a "no harm, no foul" violation of confidentiality laws.

complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[15]

67. These techniques mean that the PHI stolen in the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even though certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, they can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam medical telemarketers) over and over and over. That is exactly what is happening to Plaintiff Fox and the Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that under the circumstances of a nearly ten-fold increase in the number of scam robo-dialed calls received by Ms. Fox and other Class Members that their stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

68. Identity theft is not only impacting Plaintiff Fox and Class Members financially, but also is taking a significant emotional and physical toll. Plaintiff Fox and other Class Members, like other PHI theft victims, fear for their personal financial security and are experiencing feelings

[15] "Fullz" is fraudster speak for data that includes the *full* information of the victim, including name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge.

of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly sort of injury and harm to a Data Breach victim that is contemplated and addressed by law. As Plaintiff Fox puts it, "It feels like I'm having surgery in public."[16]

PLAINTIFF NESHEIM'S EXPERIENCE

69. Plaintiff Grant Nesheim is a resident of Mazomanie, Wisconsin. Mr. Nesheim has been a patient and user of UnityPoint and its affiliates' services since at least January, 2017. Like Ms. Fox, Mr. Nesheim received the First Notice Letter on or about April 17, 2018 and the Second Notice Letter on or about August 2, 2018 (obviously his PHI had been unlawfully viewed and accessed as well). And, like Plaintiff Fox, he has given UnityPoint every piece of PHI it has asked for during the course of his health care relationship with Defendant, including without limitation his address, phone number, health insurance information, date of birth, Social Security number, and gender as well as information on so-called intake forms describing the reasons he sought treatment.

70. Shortly after receiving the First Notice Letter, in or around May or June, 2018, Plaintiff Nesheim saw a suspicious and unauthorized charge on his credit card account. Plaintiff Nesheim confirmed the charges were not his and was forced to cancel his card and have the bank issue a new one.

[16] A 2013 survey from the Identity Theft Research Center reports that from an emotional standpoint, the impact of identity theft for some victims continues to be traumatic, as evidenced by their answers. Participant responses covered a broad range of emotions, including suicidal feelings (6.7 percent), shame or embarrassment (29.4 percent), overwhelming sadness (31.6 percent) and disbelief (41.2 percent). Much higher percentages of helplessness (50.3 percent) betrayal (50.8 percent), and rage and anger (65 percent) may be indicative of complex issues involving other types of identity theft, not just financial. Nearly 70 percent of the respondents indicated fear regarding their own personal financial security.
http://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf (last view May 4, 2018)

71. Then, on or about July 5, 2018, Plaintiff Nesheim was informed that there had been a fraudulent attempt to open an unauthorized credit card account under his name using his PHI with a different bank which he does not do business with. Since learning that he was being victimized again by Defendant's Data Breach, Mr. Nesheim has been working with that bank to make sure the account did not open and to clear his name.

72. Commencing in and around the first and second quarter of 2018, Plaintiff Nesheim, like Plaintiff Fox and the other Class Members, began to notice a tremendous increase in the amount of unsolicited auto-dialed or robo-dialed phone calls on his telephones which he simply wasn't getting before. In fact, Plaintiff Nesheim is now so inundated with the number of robo-dialed calls he is receiving (approximately 60 per month), that during the week of July 23, 2018 he took on a different work telephone number for his work phone calls. Now he has to carry two telephones, one for work and one for his older personal number, because of the overwhelmingly intrusive number of calls he is receiving.

73. Had Mr. Nesheim been informed of the true scope and extent of the Data Breach, he could and would have acted sooner and made a timely and informed decision to take action to mitigate the injury and harm he is suffering. Defendant's unreasonable delay caused by its failure to deal truthfully and in good faith with Mr. Nesheim resulted in financial fraud directly traceable to the Data Breaches.

74. For the reasons set forth above, Plaintiff Nesheim has suffered injury and harm from the Data Breaches and the misuse of his stolen PHI that is actual and ongoing, and certainly impending and imminent, including without limitation being victimized by financial identity fraud, and suffering an increase in robo-dialed scam phone calls to the point where he has been forced to change his telephone number and add another line.

PLAINTIFF DUCKLEY'S EXPERIENCE

75. Plaintiff Danielle Duckley is a resident of Silvis, Illinois. Ms. Duckley has been a patient and user of UnityPoint and its affiliates' services since at least January 1, 2010. Like Ms. Fox and Mr. Nesheim, Ms. Duckley received the Second Notice Letter on or about August 2, 2018 indicating her PHI had been unlawfully viewed and accessed. And, like Plaintiffs Fox and Nesheim, she has given UnityPoint every piece of PHI it has asked for during the course of her health care relationship with Defendant, including without limitation her address, phone number, health insurance information, date of birth, Social Security number, and gender as well as information on so-called intake forms describing the reasons she sought treatment.

76. Shortly after the Second Data Breach, Plaintiff Duckley was suddenly and inexplicably unable to log into a credit bureau account she had at Experian. Ms. Duckley called Experian and told them what was happening and changed her password to gain access to her account. After receiving the Second Notice Letter, Plaintiff Duckley informed Experian about the Second Data Breach. In response, Experian told her that the Second Data Breach had undoubtedly been the cause of her being locked out of her account due to repeated unauthorized log in attempts.

77. Since the Second Data Breach, Plaintiff Duckley, like Plaintiff Fox, Plaintiff Nesheim, and other Class Members, noticed a marked and significant increase in the amount of unsolicited auto-dialed or robo-dialed phone calls on her telephones which she wasn't getting before. Ms. Duckley, like the other Plaintiffs, is being harassed and inundated with unwanted, unsolicited, and unlawful spam and phishing emails and auto-dialed calls. These calls not only restrict Plaintiff's phone usage, but also use up amounts of Plaintiff's phone battery and the costs of the electricity needed to recharge her mobile phone. These spam emails and robo-dialed calls also cause Plaintiff annoyance, frustration, and wasted time. Plaintiff's privacy is being invaded

as a direct result of the Second Data Breach, and she and her property rights are being caused harm without her permission.

78. Plaintiff Duckley, like the other Plaintiffs, began receiving a slew of notices after the Second Data Breach notifying her or unauthorized attempts to use her password to try and sign into various online accounts she has. This too is either an attempt to victimize Ms. Duckley again by obtaining access to her online account with a "phishing email", or she is the victim of a cyber-criminal's unauthorized attempt to fraudulently gain access to her account. This increase in fraudulent activity is directly traceable to the Second Data Breach and is causing Ms. Duckley injury and harm.

79. On or about August 9, 2018, Plaintiff Duckley again looked at her Experian account. A review of her account indicated that her identity and email had been found on the dark web at a site called zomato.com. The reported date of her compromised identity found on the dark web was July 1, 2018. This reported identity theft discovered on the dark web is directly traceable to the Second Data Breach and is causing Ms. Duckley injury and harm. Had Ms. Duckley been timely informed of the true scope and extent of the Data Breach, she could and would have made a more timely and informed decision to take action to mitigate the injury and harm she is suffering. Defendant's unreasonable delay and its failure to deal truthfully and in good faith with Ms. Duckley has resulted in identity fraud traceable to the Second Data Breach.

80. For the reasons set forth above, Plaintiff Duckley has suffered injury and harm from the Second Data Breach and the misuse of her stolen PHI that is actual and ongoing, and certainly impending and imminent, including without limitation being victimized by financial identity fraud, the unauthorized attempted hacking into her Experian account, suffering an increase in robo-dialed

scam phone calls, unauthorized attempts to hack into her other online accounts, and exposure of her identity on the dark web.

PLAINTIFF KITSIS' EXPERIENCE

81. Plaintiff Kitsis is a resident of Des Moines, Iowa. Ms. Kitsis has been a patient and user of UnityPoint and its affiliates' services since at least January 1, 2010. Like the other Plaintiffs, Ms. Kitsis received the Second Notice Letter on or about August 2, 2018 indicating her PHI had been unlawfully viewed and accessed. And, like the other Plaintiffs, she has given UnityPoint every piece of PHI it has asked for during the course of her health care relationship with Defendant, including without limitation her address, phone number, health insurance information, date of birth, Social Security number, and gender as well as information on so-called intake forms describing the reasons she sought treatment.

82. Since the Second Data Breach, Plaintiff Kitsis, like the other Plaintiffs and Class Members, began to notice an increase in the amount of unsolicited auto-dialed or robo-dialed phone calls on her telephones which she wasn't getting before. Ms. Kitsis, like the other Plaintiffs, is being harassed with unwanted, unsolicited, and unlawful auto-dialed calls. These calls not only restrict Plaintiff's phone usage, but also use up amounts of Plaintiff's phone battery and the costs of the electricity needed to recharge her mobile phone. These robo-dialed calls also cause Plaintiff annoyance, frustration, and wasted time. Plaintiff's privacy is being invaded as a direct result of the Second Data Breach, and she and her property rights are being caused harm without her permission.

83. On or about August 8, 2018 Plaintiff Kitsis spoke with a UnityPoint representative who refused to give her last name, only referring to herself as Jill W. Ms. Kitsis asked Jill W. what specific information was included in her PHI that was stolen. Contrary to the description of

the stolen PHI in the Second Notice Letter received by Ms. Kitsis, Jill W. falsely stated to Plaintiff Kitsis that only "a billing statement" was involved in the theft of Ms. Kitsis' PHI. Defendant has failed to date to confirm the specific PHI of Plaintiff's that was stolen, and what other information in her medical records has been accessed without her consent, despite Plaintiff Kitsis' requests to do so.

84. Plaintiff Kitsis' PHI is extraordinarily sensitive, and its theft is not only impacting her financially, but also is taking a significant emotional and physical toll. Because of the very sensitive nature of her PHI, Plaintiff Kitsis, like other Class Members and PHI theft victims, fears for her personal financial security and safety, and is experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain. This distress goes well beyond allegations of mere worry or inconvenience, and it is exactly sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

CLASS ACTION ALLEGATIONS

85. Plaintiffs bring this action pursuant to pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of themselves and all Members of the Class and Subclasses defined as:

> ***The Wisconsin Data Breach Class***. All residents of Wisconsin whose Personal Health Information was accessed by unauthorized third parties in the First Data Breach or Second Data Breach.
>
> ***The Wisconsin Notice Letter Class.*** All residents of Wisconsin who were mailed and received the First Notice Letter or Second Notice Letter.

The Wisconsin Data Breach Class and Wisconsin Notice Letter Class are individually and collectively referred to herein as the "Wisconsin Class" or "Wisconsin Class Members".

> ***The Iowa Data Breach Class***. All resident of Iowa whose Personal Health Information was accessed by unauthorized third parties in the First Data Breach or Second Data Breach.

> ***The Iowa Notice Letter Class.*** All residents of Iowa who were mailed and received the First Notice Letter or Second Notice Letter.

The Iowa Data Breach Class and Iowa Notice Letter Class are individually and collectively referred to herein as the "Iowa Class" or "Iowa Class Members".

> ***The Illinois Data Breach Class***. All resident of Illinois whose Personal Health Information was accessed by unauthorized third parties in the First Data Breach or Second Data Breach.

> ***The Illinois Notice Letter Class.*** All residents of Illinois who were mailed and received the First Notice Letter or Second Notice Letter.

The Illinois Data Breach Class and Illinois Notice Letter Class are individually and collectively referred to herein as the "Illinois Class" or "Illinois Class Members". The Classes described in this Complaint may be jointly referred to as the "Class" and proposed members of the Classes may be jointly referred to as "Class Members."

86. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

87. Plaintiffs and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 23 of the Federal Rules of Civil Procedure.

88. **Numerosity**: The exact number of members of the Class is unknown, but is estimated to be at least 1.4 million persons at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies**.**

89. **Typicality**: Plaintiffs' claims are typical of the claims of other members of the Class in that Plaintiffs and the Class Members sustained damages all arise out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and the Class Members sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

90. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with or are antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff.

91. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. whether Defendant violated the laws asserted herein, including without limitation the Wisconsin Confidentiality of Patient Health Care Records laws, Wis. Stat. §§ 146.81, *et seq.*, Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§100.18, *et seq.*, and other federal and state statutory privacy and consumer protection laws;

b. whether Defendant had a duty to use reasonable care to safeguard Plaintiffs' and the Class Members' PHI;

c. whether Defendant breached the duty to use reasonable care to safeguard Class Members' PHI;

d. whether Defendant breached its contractual promises to safeguard Plaintiffs' and the Class Members' PHI;

e. whether Defendant was negligent *per se* in not complying with federal and state privacy laws;

f. whether Defendant had a duty to disclose the truth about the Data Breaches in connection with affected patients' PHI;

g. whether Defendant knew or should have known their practices and representations related to the Notice Letters, Data Breaches, and PHI were deceptive and unfair;

h. whether Defendant knew or should have known about the inadequacies of their date security policies and system and the dangers associated with storing sensitive PHI;

i. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class Members' PHI from unauthorized release and disclosure;

j. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and the other Class Members' PHI from unauthorized release and disclosure;

k. whether Defendant took reasonable measures to determine the extent of the Data Breaches after they were discovered;

l. whether Defendant's delay in informing Plaintiffs and the other Class Members of the Data Breaches was unreasonable;

m. whether Defendant's method of informing Plaintiffs and the other Class Members of the Data Breaches was unreasonable;

n. whether Defendant's conduct was deceptive, unfair, or unconscionable, or constituted unfair competition;

o. whether Defendant's conduct was likely to deceive a reasonable consumer;

p. whether Defendant is liable for negligence or gross negligence;

q. whether Defendant's conduct, practices, statements, and representations about the Data Breaches of the PHI violated applicable state laws;

r. whether Defendant knew or should have known their representations were false, deceptive, unfair, and misleading;

s. whether Defendant concealed material information regarding the true breadth, scope, and nature of the PHI compromised and stolen in the Data Breaches;

t. whether Plaintiffs and the Class Members were injured as a proximate cause or result of the Data Breaches;

u. whether Plaintiffs and the Class Members were damaged as a proximate cause or result of and Defendant's breaches of its contract with Plaintiffs and the Class Members;

v. whether Defendant's practices and representations related to the Data Breaches that compromised the PHI breached implied warranties;

w. whether Defendant has been unjustly enriched as a result of the conduct complained of herein;

x. what is the proper measure of damages; and

y. whether Plaintiffs and the Class Members are entitled to restitutionary, injunctive, declaratory, or other relief.

92. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of

individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

93. A class action is therefore superior to individual litigation because:

a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the Class action procedure;

b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

94. In addition to satisfying the prerequisites of Fed. R. Civ. P. 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Fed. R. Civ. P. 23(b)(2) and (3). Class certification is appropriate under Fed. R. Civ. P. 23(b)(1) or (b)(2) because:

a. the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant;

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole.

COUNT I
Negligence
On Behalf of Each Plaintiff and the Classes

95. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

96. Plaintiffs and Class Members entrusted their PHI to Defendant. Defendant owed to Plaintiffs and the other Class Members a duty to exercise reasonable care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breaches, theft, and unauthorized use, and to promptly detect attempts at unauthorized access.

97. Defendant owed a duty of care to Plaintiffs and Class Members because Plaintiffs and Class Members were foreseeable and probable victims of using email, and negligent, insecure emailing practices, to transmit and send confidential PHI, and Defendant's failure to secure the PHI. Defendant acted with wanton and reckless disregard for the security and confidentiality of

Plaintiffs' and Class Members' PHI by disclosing and providing access to this information to third parties and by failing to properly supervise the manner in which the PHI was stored, used, and exchanged.

98. Defendant owed to Plaintiffs and the Class Members a duty to notify them within a reasonable time frame of any breach to the security of their PHI under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320(d), *et seq.* ("HIPAA"), Wis. Stat. § 134.98, and other federal and state laws as referred to herein. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and the other Class Members the scope, nature, and occurrence of the Data Breaches. This duty is required and necessary in order for Plaintiffs and the other Class Members to take appropriate measures to protect their PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breaches.

99. Defendant owed these duties to Plaintiffs and the other Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and the other Class Members' personal information and PHI. Plaintiffs and the other Class Members were required to provide their personal information and PHI to Defendant in order to obtain services, and Defendant retained the information throughout Plaintiffs' and the other Class Members' use of Defendant's services.

100. The risk that unauthorized persons would attempt to gain access to the PHI and misuse was foreseeable. As the holder of vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PHI.

101. Such information is highly valuable, and Defendant is aware of numerous instances when criminals have attempted to access, and in fact have accessed PHI from Defendant, its affiliates, and others. Defendant has been targeted by criminals successfully in the past by such attempts. Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI of Plaintiffs and the other Class Members, and the importance of exercising reasonable care in handling it.

102. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PHI of Plaintiffs and the other Class Members which actually and proximately caused the Data Breaches and Plaintiffs' and the other Class Members' injury. Defendant further breached its duties by failing to provide timely and accurate notice of the Data Breaches to Plaintiffs and the other Class Members, which actually and proximately caused and exacerbated the harm from Data Breaches and Plaintiffs' and the other Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including embarrassment, humiliation, frustration, and emotional distress.

103. Defendant's breach of its common law duties to exercise reasonable care and it's failures and negligence actually and proximately caused the Plaintiffs' and other Class Members' actual, tangible injury-in-fact, and damages, including without limitation the theft of their PHI by criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted and was caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
On Behalf of Each Plaintiff and the Classes

104. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

105. Pursuant to HIPAA and applicable federal and state law as set forth herein (*e.g.,* Wis. Stat. §§ 146.81, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and the Class Members' PHI. Pursuant to applicable state laws as referred to herein, including but not limited to Wisconsin, Defendant had a duty to Plaintiffs and Class Members residing in those states to not disclose and to safeguard Plaintiffs' and Class Members' confidential PHI.

106. In addition, pursuant to Wisconsin law (Wis. Stat. §§ 134.98(3)(a)), Defendant had a duty to provide notice to Plaintiffs and the Class Member within 45 days after it learned of the Data Breaches. Further, Defendant had a duty to notify "without unreasonable delay" all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices sent to the individuals. Wis. Stat. § 134.98(2)(br).

107. In addition to violations of HIPAA and state laws, Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits "unfair . . . practices in or affecting commerce" including, as recently interpreted by the Federal Trade Commission ("FTC"), acts or practices that fail to take reasonable measures to protect customers' personal information like the PHI. Defendant violated Section 5 and similar statues by failing to employ reasonable security systems, controls and procedures to protect the PII of Plaintiffs and the other Class Members which violations constitutes negligence *per se*.

108. Defendant breached its duties under federal and state law to Plaintiffs and the Class Members by providing access, exposing, and disclosing their information to third parties, by failing to safeguard and provide adequate security for their PHI in an unreasonable manner, by failing to give timely notice to Plaintiffs and the Class Members, and by failing to the give the required information to national consumer reporting agencies without unreasonable delay. Defendant's failure to comply with these applicable laws and regulations constitutes negligence *per se*.

109. Plaintiffs and the Class Members are the individuals the federal and state statues set forth herein seek to protect. For instance, the FTC Act expressly prohibits "unfair" acts that "cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers." Similarly, the other federal and state laws referred to herein seek to protect Plaintiffs and the Class Members.

110. Additionally, the harm that has occurred to Plaintiffs and the other Class Members is the type of harm the FTC Act and other federal and state laws set forth herein were intended to prevent and remedy. The FTC and other federal and state regulatory authorities have pursued a number of enforcement actions against businesses that caused the unauthorized dissemination, collection or use of their customers' PHI and personal information as a result of the businesses' lack of reasonable and adequate security measures and practices.

111. But for Defendant's negligence *per se*, breach of their duties, and/or negligent supervision of their agents, contractors, vendors, and suppliers, Plaintiffs and the Class Members would not have suffered injury-in-fact. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of, and directly traceable to, Defendant's breach of its duties. Defendant knew or should have known that they were failing to meet their duties, and

that Defendant's breach thereof would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their confidential PHI.

112. As a direct, actual, and proximate result of Defendant' negligent conduct and/or negligence *per se*, Plaintiffs and Class Members have been injured and are entitled to damages.

COUNT III
Breach of Confidentiality of Health Records, Wis. Stat. 146.81, *et seq*.
On Behalf of Plaintiff Fox and Plaintiff Nesheim and the Wisconsin Data Breach Class

113. Plaintiff Fox and Plaintiff Nesheim (the "Wisconsin Plaintiffs") and the Wisconsin Data Breach Class Members incorporate the above allegations as if fully set forth herein.

114. Wisconsin law regarding Confidentiality of Patient Health Care Records, Wis. Stat. §§ 146.81, *et seq*., states that:

> "All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient." Wis. Stat. § 146.82(1).

115. The stolen PHI belonging to the Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members are "Health care records" under Wis. Stat. § 146.81(4).[17]

116. Defendant violated Wis. Stat. §§ 146.81*, et seq*. when it compromised, allowed access to, released, and disclosed patient health care records and PHI to third parties without the informed consent or authorization of Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members. Defendant did not and does not have express or implied consent to disclose, allow access to, or release the Wisconsin Plaintiffs' and the Wisconsin Data Breach Class Members' PHI. To the contrary, Defendant expressly undertook a duty and obligation to the Wisconsin Plaintiffs

[17] "'Patient health care records' means all records related to the health of a patient prepared by or under the supervision of a health care provider; . . ." Wis. Stat. § 146.81(4).

and the Wisconsin Data Breach Class Members when it told them their PHI would be private and secure.

117. Defendant did not disclose to or warn the Wisconsin Plaintiffs and Wisconsin Data Breach Class Members that their PHI could be compromised, stolen, released, or disclosed to third parties without their consent as a result of Defendant's computer systems and software being outdated, easy to hack, inadequate, and insecure. The Wisconsin Plaintiffs and Wisconsin Data Breach Class Members did not know or expect, or have any reason to know or suspect, that Defendant's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their PHI to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to the Wisconsin Plaintiffs and Wisconsin Data Breach Class Members, and on Defendant's website, namely that,

> "[UnityPoint] will use security procedures to protect personal information you submit to us from misuse or unauthorized disclosure. The personal information that you submit to us is stored in a *secure* database behind an electronic firewall." [*Emphasis added*.]

And,

> *"Access to the data is limited to a few computer technicians* for our site who need to maintain the database and who also use passwords for that access, as well as outside vendors who may occasionally assist us in maintaining and improving our hardware and software tools." [*Emphasis added*.]

And,

> "At UnityPoint Health, we have a compliance program that includes policies implementing patient privacy and security requirements mandated under federal and state law. We provide training to our employees on the importance of complying with these policies and regularly conduct audits to confirm the effectiveness of our privacy and security compliance policies."

118. Wis. Stat. § 146.84(1)(b) states,

> Any person, including the state or any political subdivision of the state, who violates Wis. Stat. s. 146.82 or 146.83 in a manner that is knowing and willful shall

> be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $25,000 and costs and reasonable actual attorney fees."

119. Wis. Stat. § 146.84(1)(bm) states,

> "Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. s. 146.82 or 146.83 shall be liable to *any person injured* as a result of the violation for actual damages to that person, *exemplary damages* of not more than $1,000 and costs and reasonable actual attorney fees." Wis. Stat. § 146.84(1)(bm). [*Emphasis added*.]

120. Wis. Stat. § 146.84(1)(c) states,

> "An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection."

121. Actual damages are not a prerequisite to liability for statutory or exemplary damages under Wis. Stat. § 146.81. A simple comparison of other Wisconsin statues (*e.g.*, Wis. Stat. § 134.97(3)(a) and (b), "Civil Liability; Disposal And Use" of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. § 146.84 when it explicitly did so in other privacy statutes. *See* Wis. Stat. § 134.97(3)(a) and (b).[18]

---

[18] "A financial institution, medical business or tax preparation business is liable to a person whose personal information is disposed of in violation of sub. (2) for *the amount of damages resulting from the violation.*" Wis. Stat. § 134.97(3)(a). [*Emphasis added*.]

"Any person who, for any purpose, uses personal information contained in a record that was disposed of by a financial institution, medical business or tax preparation business is liable to an individual who is the subject of the information and to the financial institution, medical business or tax preparation business that disposed of the record for *the amount of damages resulting from the person's use of the information*. This paragraph does not apply to a person who uses personal information with the authorization or consent of the individual who is the subject of the information." Wis. Stat, § 134.97(3)(b). [*Emphasis added*.]

122. Similarly, the Wisconsin Legislature made it clear that the exemplary damages referred to in Wis. Stat. § 146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statue (Wis. Stat. § 895.043(2), "Scope" of punitive damages), specifically and unequivocally excludes an award of "exemplary damages" under Wis. Stat. §§ 146.84(1)(b) and (bm) from the scope of "punitive damages" available under Section 895.043.[19] In short, exemplary damages under Wis. Stat. § 146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been "injured" as a result of a negligent data breach like the one at issue here.

123. The plain, common dictionary definition of "injure" is,

> " **injured**; **injuring** play \ˈinj-riŋ, ˈin-jə-\
> transitive verb
> **1a :** to do an injustice to **:** wrong
> **b :** to harm, impair, or tarnish the standing of
> • *injured* his reputation
> **c :** to give pain to
> • *injure* a person's pride
> **2a :** to inflict bodily hurt on
> **b :** to impair the soundness of
> • *injured* her health
> **c :** to inflict material damage or loss on."

Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/injure. *See also* footnote 5 citing Black's Online Law Dictionary, Online 2nd Ed. defining "injury" as,

> "Any wrong or damage done to another, either In his person, rights, reputation, or property. Parker v. Griswold, 17 Conn. 298, 42 Am. Dec. 739; Woodruff v. Mining Co., 18 Fed. 781; Hitch v. Edgecombe County, 132 N. C. 573, 44 S. E. 30; Macauley v. Tierney, 19 R. I. 255, 33 Atl. 1, 37 L. R.

[19] "This section does not apply to awards of double damages or treble damages, or to the award of exemplary damages under ss. 46.90 (9) (a) and (b), 51.30 (9), 51.61 (7), 55.043 (9m) (a) and (b), 103.96 (2), 134.93 (5), **146.84 (1) (b) and (bm)**, 153.76, 252.14 (4), 252.15 (8) (a), 610.70 (7) (b), 943.245 (2) and (3) and 943.51 (2) and (3). [**Emphasis added**.]

> A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of any one, whereby his body, his dignity, or his reputation is maliciously injured. Voet, Com. ad Pand. 47, t. 10, no. 1."

124. The Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PHI data between Defendant and third parties unlawful. The Wisconsin Plaintiffs and Wisconsin Data Breach Class Members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using PHI without first adequately securing or encrypting it.

125. The Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PHI in their possession or the possession of third parties and provide it to the Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members.

126. The Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members request that the Court enter an injunction ordering that Defendant:

(a) engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant’s safeguards and procedures on a periodic basis;

(b) audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

(c) conduct regular checks and tests on its safeguards and procedures;

(d) periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

(e) meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard patient PHI; and

(f) identify to each Class Member in writing with reasonable specificity the PHI and personal information of each such Class Member that was stolen in the Data Breach, including without limitation as required under Wis. Stat. § 134.98(3)(c).

127. The Wisconsin Plaintiffs and the Wisconsin Data Breach Class Members request the Court enter an order pursuant to Wis. Stat. § 146.84(1)(bm) awarding minimum statutory exemplary damages of $1,000 to each Plaintiff and each Class Member whose PHI was compromised and stolen, as well as attorneys' fees and costs.

COUNT IV
State Data Breach Notification Statutes
On Behalf of Each Plaintiff and the Classes

128. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

129. The Data Breaches constitute a breach of Defendant's computer security systems within the meaning of state data breach notifications statutes, including without limitation Wis. Stat. §§ 134.98(3)(a) and (2)(br), Ill. Comp. Stat. Ann. 530/10(a), *et seq.*, and Iowa Code Ann. §§ 715.1 and 2 (collectively referred to herein as the "State Notice Statutes"). The PHI accessed in the Data Breaches was protected and covered by the listed statutes.[20]

[20] The Data Breach notification statutes of Wisconsin (Wis. Stat. §§ 134.98(3)(a) - notice must be given within a reasonable time, not to exceed 45 days after the entity learns of the unauthorized acquisition); Illinois (815 Ill. Comp. Stat. § 530/10(a) - most expedient time possible and without

130. The PHI of Plaintiffs and the Class Members constitutes personal information as defined by the State Notice Statues.

131. Defendant unreasonably delayed notification of the Data Breaches, including the unauthorized access and theft of the PHI of Plaintiffs and the Classes after Defendant knew or should have known that the Data Breaches had occurred.

132. When the Data Breaches began, Defendant did not disclose or notify the public of the data breach. Defendant knew or should have known that the Data Breaches were occurring at the time they started, but failed to disclose their existence to the Plaintiffs, the Class Members, and the public, at that time.

133. During the time between the First Data Breach and the Second Data Breach Defendant took no action to remedy the First Data Breach or to ensure that their systems were properly protecting the PHI of Plaintiffs and the Class Members. For a period of at least 60 days following their purported discovery the Data Breaches, Defendant failed to inform Plaintiffs, the Class Members, and the public of the Data Breaches during this time even though Defendant knew or should have known of the Data Breach occurrences and the attendant unauthorized access, theft, and dissemination of Plaintiffs' and the other Class Members' PHI.

134. To this day, it is unknown whether Defendant has fixed the unreasonable security holes that led to the Data Breaches. In their Notice Letters, notices to government regulators, and in press releases, Defendant downplayed the significance of the Data Breaches and claimed that certain PHI was not stolen and that electronic medical record systems were not compromised when

---

unreasonable delay); and Iowa Code Ann. §§ 715C.1, *et seq*. - (most expeditious manner possible and without unreasonable delay) are substantially similar.

in fact they were, and that there was no evidence of misuse of any customer PHI when in fact there was.

135. Defendant failed to disclose to Plaintiffs and the other Class Members, without unreasonable delay and in the most expedient time possible, the Data Breaches and the unauthorized access and theft of the PHI when Defendant knew, should have known, or reasonably believed that such information had been compromised.[21] As a result, Plaintiffs and the other Class Members suffered the direct harm and injury-in-fact alleged above.

136. Had Defendant provided timely and accurate notice, Plaintiffs and Class Members could have taken steps to mitigate the direct harm and injury-in-fact suffered as a result of Defendant's unreasonable and untimely delay in providing notice. Plaintiffs and the Class Members could have taken other steps in efforts to avoid the direct harm and injury caused by Defendant's failure to notify.

137. As a direct and proximate result of Defendant's violations of the State Notice Statutes, Plaintiffs and the Class Members have been harmed and injured and have suffered damages as set forth above.

[21] UnityPoint is required to accurately notify Plaintiff Kitsis and Iowa Class Members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code Ann. § 715C.2(1). UnityPoint is a business that owns or licenses computerized data that includes personal information as defined by Iowa Code Ann. § 715C.2(1). Plaintiff Kitsis and Iowa Class Members' PHI includes personal information as covered under Iowa Code Ann. § 715C.2(1). Because UnityPoint was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code Ann. § 715C.2(1). Thus, by failing to disclose the Second Data Breach in a timely and accurate manner, UnityPoint violated Iowa Code Ann. § 715C.2(1).

138. Plaintiffs and the Class Members seek all remedies available under the applicable State Notice Statutes, including but not limited to damages as alleged above, equitable relief and reasonable attorneys' fees, and costs, as provided by law.

COUNT V
Invasion of Privacy
On Behalf of Each Plaintiff and the Classes

139. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

140. Defendant published private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiffs and Class Members by disclosing and exposing Plaintiffs' and Class Members' PHI to enough people through their negligent PHI security and retention practices that it is reasonably likely those facts will become known to the public, including without limitation on the dark web and elsewhere.

141. The disclosure of the PHI, including treatment information, surgical information, diagnoses, lab results, the treatment received, and the medications taken is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

142. Defendant has a special relationship with Plaintiffs and the Class Members by virtue of their provider-patient relationship, and Defendant's disclosure of personal and private information in the PHI is certain to embarrass them and offend their dignity. UnityPoint should appreciate that the cyber-criminals who stole the PHI would further sell and disclose the PHI as they are doing. That the original disclosure is devastating to the Plaintiffs and the Class Members even though it may have originally only made to one person or a limited number of cyber-criminals does not render it any less a public disclosure.

143. The tort of public disclosure of private facts is recognized in Wisconsin, Illinois, Iowa. Plaintiffs and the Class Members' private PHI was publicly disclosed by UnityPoint in the Data Breaches with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew and knows that Plaintiffs' and Class Members' PHI is not a matter of legitimate public concern. As a direct and proximate result of Defendant' conduct, Plaintiffs and Class Members have been injured and are entitled to damages. [22]

COUNT VI
Misrepresentation and Concealment
On Behalf of Each Plaintiff and the Wisconsin, Illinois, and Iowa Notice Letter Classes

144. Plaintiffs and the Wisconsin, Illinois, and Iowa Notice Letter Class Members (collectively the "Notice Class Members") incorporate the above allegations as if fully set forth herein.

145. Defendant knowingly made false and deceptive representations regarding its data security practices and policies, in its privacy statements, and elsewhere, including enumerating

[22] In Wisconsin invasion of privacy actions are governed by Wis. Stat. § 895.50, which provides in relevant part: (1) The right of privacy is recognized in this state. One whose privacy is unreasonably invaded is entitled to the following relief:....(b) Compensatory damages based either on plaintiff's loss or defendant's unjust enrichment; and(c) A reasonable amount for attorney fees.(2) In this section, invasion of privacy means any of the following:....(c) Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed. It is not an invasion of privacy to communicate any information available to the public as a matter of public record. In order to establish a cause of action for invasion of privacy under Wis. Stat. § 895.50(2)(c), a plaintiff must prove: (1) a public disclosure of facts regarding the plaintiff; (2) the facts disclosed are private facts; (3) the private matter made public is one which would be highly offensive to a reasonable person of ordinary sensibilities; and (4) the defendant acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter, or with actual knowledge that none existed.

specific uses and ways in which the PHI could be shared. Defendant additionally knowingly made false and deceptive statements in its Notice Letters and in statements and representations made to the public through press releases and on Defendant's website to cover up and conceal the breadth, scope, and nature of the Data Breaches through knowing misrepresentations and omissions of material fact.

146. On or about April 16, 2018, Defendant knowingly misrepresented the nature, breadth, scope, harm, and cost of the First Data Breach to Plaintiffs and the First Notice Class Members when RaeAnn Isaacson, Privacy Officer falsely stated on behalf of Defendant in the First Notice Letter that "The [stolen] information did not include your Social Security number", and "We have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes."

147. Defendant knowingly misrepresented in statements it made to Plaintiffs and the Notice Class Members the public on April 16, 2018 in press releases and on Defendant's website that the stolen PHI did not include affected patients' Social Security number. Defendant also knowingly made false and deceptive statements on April 16, 2018 to Plaintiffs, the Notice Class Members, and the public in press releases and on Defendant's website when it claimed Defendant had no information indicating that the stolen PHI will be used for any unintended purposes. Defendant knows that stolen PHI will be used for unintended purposes.

148. On April 16, 2018, in the First Notice Letter, in press releases, and on Defendant's website, Defendant omitted the material fact that patients' Medicare numbers, and therefore Social Security numbers, are included in the compromised and stolen PHI. Defendant further knew, or should have known, it possessed information that makes it highly likely the PHI will be used for an unintended purpose. Defendant knowingly, intentionally, and recklessly made these false

statements in an effort to minimize and conceal the harm and injury-in-fact to Plaintiffs and the Notice Class Members caused by the First Data Breach.

149. On or about July 30, 2018, Defendant knowingly misrepresented the nature, breadth, scope, harm, and cost of the Second Data Breach to Plaintiffs and the Notice Class Members when RaeAnn Isaacson, Privacy Officer falsely stated on behalf of Defendant in the Notice Letter that "We want to assure you that our electronic medical record and patient billing systems were not impacted by this attack". [Underline in original.]

150. These knowing misrepresentations and omissions were intended to: (a) conceal, minimize, and obfuscate the true breadth, scope, and nature of the Data Breaches; (b) delay the notification of an investigation into the amount of liability and cost Defendant is legally responsible for to Plaintiffs and the Notice Class Members; and (c) induce Plaintiffs, the Notice Class Members, and the public to continue to use Defendant's services and/or increase consumption of Defendant's services.

151. Defendant's misrepresentations and omissions about the stolen Social Security numbers, likely use of the stolen PHI, and the compromise of and impact on electronic medical records systems were untrue. Defendant made the representations knowing they were untrue, or recklessly, without caring whether they were true or false. Defendant made these misrepresentations with intent to defraud and to induce Plaintiffs and the Notice Class Members to rely and act upon them. Plaintiffs and the Notice Class Members believed the statements to be true and relied on them to their detriment. To this day, Defendant has not told Plaintiffs or the Notice Class Members the truth about the Data Breaches.

152. Plaintiffs allege the ***who*** (Defendant itself and its Privacy Officer, RaeAnn Isaacson), ***what***, ***where*** (Defendant knowingly made false and deceptive statements to Plaintiffs

and Notice Class Members when it stated in the First Notice Letter (*where*) that the stolen PHI did not include Social Security numbers (*what*), and in the First Notice Letter and to the public in press releases and on Defendant's website (*where*) when it claimed UnityPoint had no information indicating that the stolen PHI will be used for any unintended purposes (*what*), and when it claimed in the Second Notice Letter (*where*) that electronic medical record systems were not impacted (*what*)), ***when*** (on or about April 17, 2018 and July 30, 2018), and ***why*** (in an effort to minimize and conceal the harm and injury-in-fact to Plaintiffs and the Notice Class Members caused by the Data Breaches and induce them to continue to use Defendant's services) of Defendant's misrepresentations and concealment.

153. As a result of Defendant's false and misleading statements, Plaintiffs and the other Notice Class Members have suffered additional pecuniary loss and injury-in-fact, including without limitation lost benefit of their bargain, lost value of their PHI, and consequential injury from the lost time and money incurred to mitigate and remediate the effects of the Data Breaches, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT VII
Breach of Contract
On Behalf of Each Plaintiff and the Classes

154. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

155. Defendant entered into binding and enforceable contracts with Plaintiffs and the other Class Members supported by consideration, including the payment for services by Plaintiffs and the Class Members. These contracts include terms covering privacy and limiting the use and sharing of Plaintiffs' and the other Class Members' PHI. Plaintiffs and the other Class Members

bargained for an adequate level of security and reasonable care with respect to the use, storage, and sharing of their PHI.

156. These contracts incorporated Defendant's privacy polices wherein Defendant promised to protect the privacy of Plaintiffs' and Class Members' personal information in accordance with federal and state privacy laws, as well as their own privacy policies. Specifically, and without limitation, in a written document provided to Plaintiffs and Class Members in connection with their health care services, and on Defendant's website, Defendant stated,

> "USES AND DISCLOSURES REQUIRING YOUR AUTHORIZATION. There are many uses and disclosures we will make only with your written authorization. These include: • Uses and Disclosures Not Described Above. We will obtain your authorization for uses and disclosures of your health information that are not described in the Notice above.
>
> NOTICE IN THE CASE OF BREACH. You have the right to receive notice of an access, acquisition, use or disclosure of your health information that is not permitted by HIPAA, if such access, acquisition, use or disclosure compromises the security or privacy of your PHI (we refer to this as a breach). We will provide such notice to you without unreasonable delay but in no case later than 60 days after we discover the breach.
>
> WHO WILL FOLLOW THESE PRIVACY PRACTICES? The health care organizations that are a part of UnityPoint Health have collectively formed an Affiliated Covered Entity or "ACE" under the HIPAA regulations for purposes of HIPAA compliance. A full list of organizations in the UnityPoint Health ACE, called "Affiliates" are listed in Appendix A to this Notice. Our rules to protect your privacy will be followed by all workforce members of the site where you are being treated, as well as physicians and other health care practitioners with permission to provide services at our sites who are independent of any UnityPoint Health Affiliate (together called "the UnityPoint Health ACE" in this Notice).
>
> WHAT HEALTH INFORMATION IS COVERED UNDER THIS NOTICE? This Notice covers health information at the UnityPoint Health ACE that may be written (such as a hard copy medical record file), spoken (such as physicians discussing treatment options), or electronic (such as billing records kept on a computer).
>
> **Information Security**
>
> We will use security procedures to protect personal information you submit to us from misuse or unauthorized disclosure. The personal information that you submit

> to us is stored in a secure database behind an electronic firewall. You can access your personal information only by using a password. We encourage you to change your password regularly and not to share it with anyone.
>
> Access to the data is limited to a few computer technicians for our site who need to maintain the database and who also use passwords for that access, as well as outside vendors who may occasionally assist us in maintaining and improving our hardware and software tools.
>
> **Patient Privacy at UnityPoint Health**
>
> Protecting the privacy of our patients' information is a key part of our goal to provide the best outcome for every patient every time. Across the United States, the privacy of patients' health information is protected by a federal law and regulations (commonly referred to as "HIPAA") that establish minimum standards for maintaining the privacy and security of patients' information. In addition, the states where we treat our patients also have state laws that provide additional protections for certain types of health information. At UnityPoint Health, we have a compliance program that includes policies implementing patient privacy and security requirements mandated under federal and state law. We provide training to our employees on the importance of complying with these policies and regularly conduct audits to confirm the effectiveness of our privacy and security compliance policies."

157. It was a violation of UnityPoint's privacy covenants, warranties, and promises to disclose Plaintiffs' and Class Members' highly confidential PHI in the manner described above. As a result of Defendant's breach of contract, Plaintiffs and Class Members did not receive the full benefit of their bargain and instead received services that were less valuable than described in their contracts.

158. As part of the contract between Defendant and Plaintiffs and the Class Members, Defendant offered to provide health care and health care related services in exchange for their business and payments from Plaintiffs and the Class Members or their insurers on their behalf, Defendant promised: (a) "[We] will protect your medical records and privacy"; (b) to provide notice of the Data Breach to Plaintiffs and the Class Members without unreasonable delay; (c) that their rules to protect Plaintiffs and the Class Members' privacy will be followed by all workforce

members of the site where they are being treated; (d) it will use security procedures to protect personal information which Plaintiffs and the Class Members submit to it from misuse or unauthorized disclosure; (e) that the personal information that Plaintiffs and the Class Members submit to it is stored in a secure database behind an electronic firewall; (f) that access to PHI is limited to a few computer technicians as well as outside vendors who may occasionally assist it in maintaining and improving our hardware and software tools; and (g) that it has a compliance program that includes policies implementing patient privacy and security requirements mandated under federal and state law.

159. UnityPoint also agreed to provide its health care services in a professional manner and only to share it with authorized employees as part of their work to support patient care. Implicit in performing these contractual duties is an obligation to reasonably safeguard its systems and data from cyberattack, including phishing attacks, and data breaches like the Data Breaches in this instance, which can and have caused harm and injury to Plaintiffs and the Class Members.

160. Plaintiffs and Class Members accepted UnityPoint's offer and went to, and paid, Defendant for their health care services. Plaintiffs and the Class Members contracted for and expected to receive the privacy benefits in accordance with the terms and warranties set forth above. Defendant breached the privacy obligations under its contract as set forth above and Plaintiffs and the Class Members have been injured and damaged as a result thereof.

161. Plaintiffs and the other Class Members performed their obligations under the agreements. Defendant violated the terms of the contract by disclosing and allowing unauthorized access to Plaintiffs' and the other Class Members' PHI for unauthorized purposes without first obtaining Plaintiffs' or the other Class Members' consent, or encrypting or otherwise protecting the information in a form which could not reasonably be used to identify them.

162. Defendant breached its contracts with Plaintiff and Class Members by failing to reasonably safeguard its systems and data from the Data Breaches. Defendant violated the terms of the contract by failing to take appropriate measures to protect Plaintiffs' and the other Class Members' personal information in accordance with its promises and representations. Defendant violated the agreement by failing to comply with applicable laws regarding the access, correction, and/or deletion of PHI, and notification to affected persons, including without limitation, HIPAA, the Wisconsin Health Information Privacy laws, the Wisconsin Security Breach Notification, and the other state laws set forth herein. Plaintiffs and Class Members have been injured as a result of Defendant's breach of contract and are entitled to damages.

163. As a result of Defendant's unlawful misconduct and breach of its contract with Plaintiffs and the Class Members, Plaintiffs and the Class Members have suffered additional pecuniary loss and injury-in-fact, including without limitation the improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT VIII
Breach of Implied Covenant of Good Faith and Fair Dealing
On Behalf of Each Plaintiff and the Classes

164. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

165. The law implies a covenant of good faith and fair dealing in every contract. Defendant entered into a contract with Plaintiffs and the other Class Members, which includes terms covering privacy and limiting the use and sharing of Plaintiffs' and the other Class Members' PHI.

166. Plaintiffs and the other Class Members performed their duties under the agreements. Defendant's unlawful and bad faith conduct, as described above, constitutes a breach of the implied covenant of good faith and fair dealing.

167. As a result of Defendant's unlawful misconduct and its breach of the covenant of good faith and fair dealing owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members have suffered additional pecuniary loss and injury-in-fact, including without limitation lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breaches, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT IX
Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§100.18, *et seq.*
On Behalf of Each Plaintiffs Fox and Nesheim and the Wisconsin Data Breach Class and the Wisconsin Notice Class

168. Wisconsin Plaintiffs Fox and Nesheim and the Wisconsin Data Breach Class Members and Wisconsin Notice Class Members (collectively the Wisconsin Data Breach Class Members and Wisconsin Notice Class Members are referred to herein as the "Wisconsin Class" or "Wisconsin Class Members") incorporate the above allegations as if fully set forth herein.

169. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"),[23] which provides that no,

> "firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

[23] The consumer protection laws of Wisconsin (Wis. Stat. § 100.18, *et seq.*) and Illinois (815 ILCS § 505/1, *et seq*. and ILCS § 510/2, *et seq*., are substantially similar.

The Wisconsin Plaintiffs and the Wisconsin Class Members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

170. Defendant deliberately engaged in deceptive and unlawful practices on April 16, 2018 when it issued public announcements, statements, and representations, including in press releases, on Defendant's website, and in the First Notice Letter, in violation of Wisconsin law by representing to the Wisconsin Plaintiffs and the Wisconsin Class Members and the public that the PHI information compromised and stolen in the First Data Breach did not include affected patients' Social Security number, when it fact Defendant knew that it does.

171. Defendant deliberately engaged in deceptive and unlawful practices on July 30, 2018 when it issued announcements, statements, and representations, including in press releases, on Defendant's website, and in the Second Notice Letter, in violation of Wisconsin law by representing to the Wisconsin Plaintiffs, the Wisconsin Class Members, and the public that "We want to assure you that our electronic medical record and patient billing systems were not impacted by this attack" when in fact, they had information and knowledge to the contrary. [Underline in original.]

172. Defendant further violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, so as to safeguard PHI from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the

inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the First Data Breach to enact reasonable security practices to safeguard its systems and data from cyberattacks like the Data Breaches.

173. The purpose of Defendant's misrepresentations set forth herein was to minimize the harm and injury-in-fact Wisconsin Plaintiffs and the Wisconsin Class Members are facing caused by the Data Breach, and therefore increase the sales and use of Defendant's goods and services.

174. Defendant knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breaches and theft was high. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Wisconsin Plaintiffs and the Wisconsin Class.

175. The Wisconsin Plaintiffs and the Wisconsin Class Members relied upon Defendant's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

COUNT X
Illinois Uniform Deceptive Trade Practices Act, ILCS 510/2 *et seq*.
On Behalf of Plaintiff Duckley and the Illinois Data Breach Class and the Illinois Notice Class

176. Plaintiff Duckley and the Illinois Data Breach Class Members and Illinois Notice Class Members (collectively the Illinois Data Breach Class Members and Illinois Notice Class

Members are referred to herein as the "Illinois Class" or "Illinois Class Members") incorporate the above allegations as if fully set forth herein.

177. Defendant, operating its business in Illinois, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. §§ 510/2(a)(5) and(7), including without limitation by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack like the Data Breaches to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the First Data Breach to enact reasonable security practices to safeguard its systems and data from the cyberattacks like the Second Data Breach.

178. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff Duckley and the Illinois Class suffered harm and injury-in-fact, as set forth herein. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that Plaintiff Duckley and the Illinois Class

could not reasonably avoid, and this substantial injury outweighed any benefits to consumers or to competition.

179. Defendant knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breaches and theft was high. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Duckley and the Illinois Class.

180. Plaintiff Duckley and the Illinois Class seek relief for violations of 815 Ill. Comp. Stat. § 510/2, *et seq*., including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

COUNT XI
Illinois Consumer Fraud Act, ILCS 505/2, *et seq*.
On Behalf of Plaintiff Duckley and the Illinois Data Breach Class and the Illinois Notice Class

181. Plaintiff Duckley and the Illinois Class incorporate the above allegations as if fully set forth herein.

182. Defendant, operating its business in Illinois, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. §§ 505/2, *et seq*., including without limitation by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack like the Data Breaches to prevent infiltration of the security system so

as to safeguard PHI from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the First Data Breach to enact reasonable security practices to safeguard its systems and data from the cyberattacks like the Second Data Breach.

183. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff Duckley and the Illinois Class suffered harm and injury-in-fact, as set forth herein. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that Plaintiff Duckley and the Illinois Class could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

184. Defendant knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breaches and theft was high. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Duckley and the Illinois Class.

185. Plaintiff Duckley and the Illinois Class seek relief under 815 Ill. Comp. Stat. § 505/10a, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

COUNT XII

Private Right of Action for Iowa Consumer Frauds Act, Iowa Code § 714H, *et seq*.
On Behalf of Plaintiff Kitsis and the Iowa Data Breach Class and the Iowa Notice Class

186. Plaintiff Kitsis and the Iowa Data Breach Class Members and Iowa Notice Class Members (collectively the Iowa Data Breach Class Members and Iowa Notice Class Members are referred to herein as the "Iowa Class" or "Iowa Class Members") incorporate the above allegations as if fully set forth herein.

187. The Iowa Private Right of Action for Consumer Frauds Act prohibits unfair and deceptive trade practices in the sale, lease, or advertisement of a product or service, and in the solicitation of charitable contributions. The Iowa Private Right of Action for Consumer Frauds Act's purpose is to protect consumers against these unfair and deceptive business practices and provide efficient and economical procedures to secure such protection.

188. Defendant operating in Iowa has violated the Act by engaging in the unfair and/or deceptive acts and practices described herein, which were and are intended to and did and do result in the purchase of Defendant's products and services by consumers, including Plaintiff Kitsis and Iowa Class Members.

189. Plaintiff has provided the requisite notice to the Iowa Attorney General pursuant to Iowa Code § 714H.7.

190. As a result of Defendant's unfair and deceptive business practices, Plaintiff Kitsis and the Iowa Class Members have lost money or property and therefore seek their actual damages. Plaintiff Kitsis and the Iowa Class Members also seek and are entitled to an order enjoining Defendant from continuing to engage in the unfair and deceptive business practices alleged herein.

COUNT XIII
Unjust Enrichment (In the alternative to Breach of Contract if Required by Law)
On Behalf of Each Plaintiff and the Classes

191. Plaintiffs plead this count in the alternative to their other Counts, including for the Wisconsin Plaintiffs and Wisconsin Class Members for Breach of Contract, where required by law, and incorporate the above allegations as if fully set forth herein.[24]

192. Plaintiffs and the other Class Members conferred non-gratuitous monetary benefits on Defendant in the form of money paid for the purchase of services from Defendant. Defendant appreciates or has knowledge of the benefits conferred directly upon them by Plaintiffs and the other members of the Class.

193. Defendant knew or should have known about the Data Breaches, and but for their own inadequate security practices, would have known about the Data Breaches on the original dates of occurrence and its own course of conduct in covering it up.

194. Had Plaintiffs and the other Class Members timely been alerted to, or known about the Data Breaches on the dates of occurrence, they would not have used Defendant's services as they did and conferred upon Defendant monetary benefits as they did.

195. The financial benefits of money paid by Plaintiffs and the other Class Members and the profits derived therefrom are a direct and proximate result of Defendant's unlawful and negligent practices and Defendant's failure to timely notify Plaintiffs and the other Class Members of the Data Breaches. These financial benefits rightfully belong to Plaintiffs and the other Class Members and it would be inequitable under unjust enrichment principles for Defendant to retain any of these benefits they would not have received but-for their illegal and uncaring conduct.

[24] Unjust enrichment laws are consistent across jurisdictions. *See In re Target Corp. Data Sec. Breach Litig.*, MDL 14-md-2522, 2014 WL 7192478, at *22 (D. Minn. Dec. 18, 2014).

There is no adequate remedy available to Plaintiffs and the Class Members at law.

196. As such, Defendant should be compelled to disgorge all inequitable proceeds to Plaintiffs and the other Class Members by way of a common fund for their benefit. A constructive trust should be imposed to recoup the inequitable sums received by Defendant and traceable to Consumer Plaintiffs and the other Class members. Plaintiffs and the other Class Members are therefore entitled to restitution, disgorgement, and imposition of a constructive trust.

COUNT XIV
Declaratory Relief
On Behalf of Each Plaintiff and the Classes

197. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

198. Defendant acted or refused to act on grounds that apply generally to Plaintiffs and the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole within the meaning of Fed. R. Civ. P. 23.

199. Plaintiffs seeks a declaration that Defendant's acts and omissions as alleged herein violates applicable state law, including without limitation the WDTPA, as well as such other and further relief as may follow from the entry of such a judgment and request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PHI data between Defendant and third parties unlawful.

200. Plaintiffs and the Class Members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using PHI without first adequately securing or encrypting it.

201. Plaintiffs and the Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PHI in their possession or the possession of third parties and provide it to Plaintiffs and the Data Breach Class Members.

202. Plaintiffs and the Data Breach Class Members request that the Court enter an injunction ordering that Defendant:

(a) engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant's safeguards and procedures on a periodic basis;

(b) audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

(c) conduct regular checks and tests on its safeguards and procedures;

(d) periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

(e) meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard patient PHI; and

(f) identify to each Class Member in writing with reasonable specificity the PHI and personal information of each such Class Member that was stolen in the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, requests the Court:

A. Certify this case as a Class action on behalf of the Class defined above, appoint Yvonne Mart Fox, Grant Nesheim, Danielle Duckley, and Shelley Kitsis as Class representatives, and appoint the Law Office of Robert L. Teel as Class counsel;

B. Declare that Defendant is financially responsible for notifying all Class Members of the false and untrue nature of the Notice Letters in connection with the Data Breaches and stolen PHI and provide them full, fair, adequate, and truthful notice thereof;

C. Award declaratory and other equitable relief, including rescission, as is necessary to protect the interests of Plaintiffs and the Class Members;

D. Award injunctive relief as is necessary to protect the interests of Plaintiffs and the Class Members;

E. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PHI;

F. Enter an award in favor of Plaintiffs and the Class Members that includes compensatory, exemplary, punitive damages, and statutory damages, including pre and post interest thereon, in an amount to be proven at trial;

G. Award restitution and damages to Plaintiffs and the Class Members in an amount to be determined at trial;

H. Order disgorgement of Defendant's unjustly acquired revenue, profits, and other benefits resulting from their unlawful conduct for the benefit of Plaintiffs and the Class Members in an equitable and efficient manner determined by the Court;

I. Order the imposition of a constructive trust upon Defendant such that its enrichment, benefit, and ill-gotten gains may be allocated and distributed equitably by the Court to and for the benefit of Plaintiffs and the Class Members.

J. Enter an award of attorneys' fees and costs, as allowed by law;

K. Enter an award of pre-judgment and post-judgment interest, as provided by law;

L. Grant Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

M. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: August 13, 2018

/s/ Robert L. Teel

Robert L. Teel (Bar ID 127081)
LAW OFFICE OF ROBERT L. TEEL
lawoffice@rlteel.com
1425 Broadway, Mail Code: 20-6690
Seattle, Washington 98122
Telephone: 866.833.5529
Facsimile: 855.609.6911

Attorney for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

YVONNE MART FOX and GRANT NESHEIM, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

IOWA HEALTH SYSTEM, doing business as UNITYPOINT HEALTH, an Iowa non-profit corporation,

Defendant.

Case No.: 18-cv-327

CERTIFICATE OF SERVICE

CERTIFICATE OF SERVICE

I am a resident of the State of Washington, over the age of eighteen years, and not a party to the within action. My business address is Robert L. Teel, 1425 Broadway, Mail Code: 20-6690, Seattle, Washington 98122. On August 13, 2018, I served the following document(s) by Notice of Electronic Filing, which is automatically generated by the CM/ECF system at the time the document listed above was filed with this Court, to lead counsel listed by CM/ECF as "ATTORNEY TO BE NOTICED."

SECOND AMENDED CLASS ACTION COMPLAINT

I declare under penalty of perjury under the laws of the United States that the above is true and correct.

DATED: August 13, 2018

/s/ Robert Teel

Robert Teel
LAW OFFICE OF ROBERT L. TEEL
1425 Broadway, Mail Code: 20-6690
Seattle, Washington 98122
lawoffice@rlteel.com
Telephone: (866) 833-5529
Facsimile: (855) 609-6911

Attorney for Plaintiffs and the Proposed Class