UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

ALEXSIS WEBB and MARSCLETTE CHARLEY, on behalf of themselves and all others similarly situated, Plaintiffs, v. INJURED WORKERS PHARMACY, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Alexsis Webb and Marsclette Charley ("Plaintiffs"), through their attorneys and on behalf of themselves and the proposed class defined below, bring this Class Action Complaint against the Defendant, Injured Workers Pharmacy, LLC ("IWP" or "Defendant"), alleging as follows:

NATURE OF THE ACTION

1. In January 2021, IWP, a home delivery pharmacy service, lost control over 75,700 patients' highly sensitive personal records in a data breach by cybercriminals ("Data Breach").

2. As evidenced by the Data Breach carrying on undetected for four months, IWP had no means to discover and prevent data breaches from happening—allowing hackers to pilfer patients' sensitive information.

3. In May 2021—after IWP finally discovered the breach—IWP did not immediately warn or notify its patients that hackers had accessed their highly sensitive data. Instead, IWP initiated a seven month "investigation," denying patients an opportunity to proactively mitigate the Data Breach's impact on them.

4. In that time, IWP also rushed to implement new data security safeguards, requiring its

employees "to complete IT security training" and implement "reasonable physical, technical, and administrative safeguards"—safeguards that should have been in place *before* the Data Breach.

5. Indeed, following the Data Breach, IWP developed an "Ethics & Compliance Statement" for its workforce, designating "Data Privacy and Security" as one of its six "core values."[1]

6. After IWP's "investigation" inexplicably dragged on for seven months, IWP finally disclosed the Data Breach to its patients. But in its Breach Notice, IWP downplayed the Data Breach's severity and the threat it posed to patients, claiming it had "no indication that [patient] information has been misused in relation to this event," even though cybercriminals had unfettered access to patient information for *four months*. A true and correct copy of the Breach Notice is attached hereto as **Exhibit A**.[2]

7. IWP's failure to timely detect and report the Data Breach has made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their personally identifiable information ("PII").

8. Indeed, IWP did not start notifying victims of the Data Breach until February 3, 2022—nearly nine months after IWP first discovered the Data Breach and almost thirteen months after the Data Breach happened.

9. IWP's failure to protect patients' PII and adequately warn them about the Data Breach violates Massachusetts law, harming thousands of current and former IWP patients.

10. IWP knew or should have known that each victim of the Data Breach was entitled to prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

---

[1] *See* IWP's Ethics and & Compliance Statement, https://www.iwpharmacy.com/ethics-compliance (last visited May 12, 2022).

[2] Breach Notice obtained from the website of the office of the Vermont Attorney General, https://ago.vermont.gov/blog/2022/02/03/injured-workers-pharmacy-data-breach-notice-to-consumers/ (last visited May 11, 2022)

11. Upon information and belief, the stolen PII included, at least, patients' names and social security numbers.

12. Upon information and belief, IWP has not offered complimentary credit monitoring and identity protection services to all Data Breach victims and has instead put the onus on victims, providing them with instructions to monitor their own credit reports. Exh. A.

13. IWP's misconduct has injured the Plaintiffs and members of the proposed Class in at least the following ways: (i) the lost or diminished value of their PII; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive PII.

14. Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach. Defendant's failure to detect the Data Breach for almost four months underscores the out-of-date security practices and procedures it had in place before and during the Data Breach. And when the Data Breach was finally discovered, Defendant failed to provide adequate or timely notice to the Data Breach victims. Indeed, it took IWP nearly nine months from the date of discovery to start notifying victims of the Data Breach.

15. Plaintiffs and members of the proposed Class therefore bring this lawsuit seeking damages and relief for Defendant's actions.

THE PARTIES

16. Plaintiff, Alexsis Webb, is a resident and citizen of Ohio. Ms. Webb intends to remain domiciled in Ohio indefinitely, is registered to vote in the state, and maintains her true, fixed, and permanent home in Ohio. Ms. Webb is a former IWP patient and her PII was compromised by the Data Breach.

17. Plaintiff, Marsclette Charley, is a resident and citizen of Georgia. Ms. Charley intends to remain domiciled in Georgia indefinitely, is registered to vote in the state, and maintains her true, fixed, and permanent home in Georgia. Ms. Charley is a current IWP patient and her PII was compromised by the Data Breach.

18. Defendant IWP is a Massachusetts limited liability company. IWP is registered to do business in the state of Massachusetts with its principal place of business located at 300 Federal St., Andover, Massachusetts 01810.

JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action in which the amount in controversy exceeds $5 million, exclusive of costs and interest, there are more than 100 members in the proposed class, and at least one class member is a citizen of a different state than IWP, establishing minimal diversity.

20. This Court has personal jurisdiction over IWP because it is organized in Massachusetts and its headquarters is in Andover, Massachusetts.

21. Venue is proper in this Court under 28 U.S.C. §§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because IWP conducts business in this District.

COMMON FACTUAL ALLEGATIONS

A. Injured Workers Pharmacy's Failure to Prevent the Data Breach

22. Plaintiffs and members of the proposed Class are IWP's current and former patients.

23. To receive IWP's pharmaceutical services, IWP requires its patients to provide their PII.

24. IWP acquires and maintains records of its patients' information, including their full names and Social Security numbers. These records are stored on IWP's computer systems.

25. Upon information and belief, IWP also maintains records of its patients' financial account information, credit-card information, dates of birth, prescription information, diagnosis information, treatment information, treatment providers, health insurance information, medical information, and Medicare/Medicaid ID numbers, in the ordinary course of business.

26. IWP represented to its patients that it would keep their PII secure through its Privacy Policy and other disclosures.

27. In January 2021, hackers infiltrated IWP's patient records systems, giving hackers unfettered access to patient PII.

28. Because IWP had no means to prevent, detect, or stop a data breach before cybercriminals could access PII, hackers were able to access PII undetected for four months.

29. On or about May 11, 2021, IWP finally discovered that the PII of its former and current patients was compromised.

30. IWP acknowledge it had inadequate security measures in place to protect the PII. In response to the Data Breach, IWP claims it "reset passwords to impacted accounts, and investigated and remediated the event. [IWP] also took action to further enhance [its] security measures already in place to protect [its] email systems and data." Exh. A.

31. IWP's Breach Notice omits the size and scope of the breach. IWP has demonstrated a pattern of providing inadequate notices and disclosures regarding the Data Breach.

32. Upon information and belief, the Data Breach has impacted at least 75,000 IWP patients.

33. Upon information and belief, IWP failed to adequately train its employees on even basic cybersecurity protocols before the Data Breach, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of Multi-Factor Authentication for all users;

b. Locking, encrypting and limiting access to computers and files containing sensitive information;

c. Implementing guidelines for maintaining and communicating sensitive data;

d. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

e. Providing focused cybersecurity awareness training programs for employees.

34. Following the Data Breach, IWP implemented new security safeguards to prevent and mitigate data breaches—measures that should have been in place *before* the Data Breach.

35. In July 2021, two months after the Data Breach, IWP revised its Privacy Policy to explain that "IWP seeks to use reasonable physical, technical, and administrative safeguards designed to protect PII against accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use."[3] Exh. B.

36. IWP also implemented a company-wide Ethics & Compliance Statement, which named data security as a "core value":[4]

Data Privacy and Security

IWP is also committed to protecting personal data. Our Privacy Policy defines our privacy standards and guides and underscores our commitment to the protection and security of personal and patient health information. To support this commitment, all IWP employees are required to complete IT security training.

37. IWP's failure to implement these "reasonable" safeguards before the Data Breach demonstrates its negligence in allowing the Data Breach to happen.

---

[3] The Privacy Policy is inexplicably silent on IWP's requirements under U.S. law to notify patients if their PII has been compromised.

[4] *See* IWP's Ethics and & Compliance Statement, https://www.iwpharmacy.com/ethics-compliance (last visited May 12, 2022).

38. Indeed, IWP's negligent conduct caused the Data Breach. IWP violated its obligation to implement best practices and comply with industry standards concerning computer system security. IWP failed to comply with security standards and allowed its patients' PII to be accessed and stolen—for nearly four months—by failing to implement security measures that could have prevented, mitigated, or detected the Data Breach.

39. IWP ultimately admitted to the Data Breach on or about February 3, 2022—nearly two months after concluding its investigation. IWP has failed to justify the delays in notifying Data Breach victims.

40. Upon information and belief, IWP notified victims of the Data Breach that their PII was accessed by unauthorized third parties via notice letters resembling the attached Breach Notice obtained from the website of the office of Vermont's Attorney General. Exh. A.

41. IWP ominously warned Plaintiffs and members of the Class to "remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring [their] credit reports for suspicious activity and to detect errors." Exh. A.

42. IWP also suggested that Plaintiffs and members of the Class call the three credit-reporting bureaus to place "fraud alerts" or "credit freezes" on their credit reports. Exh. A.

43. What IWP did not do is provide credit monitoring or other support services to all victims of the Data Breach. Rather, IWP provides general instructions to victims to mitigate the consequences of IWP's negligence in allowing the Data Breach to occur, and its failures to detect the same for nearly four months.

44. The Breach Notice also fails to explain why it took IWP nearly nine months to notify victims after discovering the Data Breach.

45. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed.

46. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

47. Defendant knew or should have known its security systems were inadequate, particularly in light of the prior data breaches experienced by similar companies, and yet Defendant failed to take reasonable precautions to safeguard Plaintiff's and Class Members' PII.

48. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs.

49. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound emails using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed, and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with the least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

50. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….
- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it….
- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….

51. To prevent and detect cyber-attacks attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- Secure internet-facing assets
- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;
- Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as a potential full compromise;
- Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

- Apply the principle of least-privilege
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;
- Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

52. Juxtaposed against the basic and inexpensive security measures Defendant was required to implement are the immediate, substantial, and long-lasting harms that Plaintiff and Class Members will suffer due to Defendant's conduct.

B. Plaintiffs and the Proposed Class Face Significant Risk of Identity Theft

53. Plaintiffs and members of the proposed Class have suffered injuries from the misuse of their PII that can be directly traced to Defendant.

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

55. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[5]

56. As a result of IWP's failures to prevent, timely detect, and report the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of IWP and is subject to further breaches so long as IWP fails to undertake the appropriate measures to protect the PII in their possession.

[5] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited May 11, 2022).

57. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[6]

58. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII 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.

59. Social numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

60. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[6] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited April 18, 2022).

[7] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 10, 2022).

61. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

62. Further, it can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

63. One such example of criminals using PII for profit is the development of "Fullz" packages.[9]

64. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

65. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher

---

[8] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited May 10, 2022).

[9] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the 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 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. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited May 11, 2022).

price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

66. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

67. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and the Class that their PII had been stolen.

68. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

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

70. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

71. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[10]

72. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[11] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[12]

73. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[13] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

---

[10] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited May 11, 2022).

[11] *Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 11, 2022).

[12] *Id.*

[13] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Jan. 18, 2022).

74. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

75. These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. IWP thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

76. IWP disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, IWP opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial

accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

77. IWP'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 privacy, and has exposed the PII of Plaintiffs and thousands of members of the proposed Class to unscrupulous operators, con artists and outright criminals.

78. IWP's failure to properly and promptly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

79. Upon information and belief, IWP knew the severity of the Data Breach but chose to downplay the Data Breach's impact. In its Breach Notice, IWP states that "there is no indication that [patients'] information has been misused in relation to" the Data Breach. Ex. A.

80. In the same Breach Notice, IWP also acknowledged that its systems, policies, and procedures were not adequate at the time of the Data Breach, thus subjecting patients' PII to exposure by an unauthorized party. *Id.*

81. As a result, whether or not IWP had immediate evidence of misuse of the accessed PII, the Data Breach resulted in at least one unauthorized user viewing and accessing patients' PII and thus it was, for all practical purposes, stolen and misused.

PLAINTIFFS' EXPERIENCES

Plaintiff Webb

82. Plaintiff Webb received pharmaceutical services from IWP between 2017 and 2020.

83. As a condition of receiving prescriptions and IWP's services, IWP required Ms. Webb to provide it with her PII.

84. Ms. Webb provided IWP with her PII in order to purchase and receive prescription deliveries from IWP. Ms. Webb would not have provided her PII to IWP had she known that IWP would not protect it as promised.

85. On or about February 3, 2022, Ms. Webb received notice from IWP that her PII was compromised by the Data Breach.

86. In response, Ms. Webb has spent considerable time and effort monitoring her accounts to protect herself from additional identity theft. Ms. Webb fears for her personal financial security and uncertainty over what information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

87. Upon information and belief, Ms. Webb's sensitive information, including her name and Social Security number, has already been used by an unauthorized individual.

88. Ms. Webb has expended considerable time communicating with the Internal Revenue Service to resolve issues related to her 2021 tax returns filed by an unknown and unauthorized third-party.

89. Ms. Webb is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

90. Ms. Webb stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

91. Ms. Webb suffered actual injury in the form of damages to and diminution in the value of her PII --a form of intangible property that Ms. Webb entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

92. Ms. Webb has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Charley

93. Plaintiff Charley is a current IWP patient and has received pharmaceutical services from IWP since 2016.

94. As a condition of receiving prescriptions and IWP's services, IWP required Ms. Charley to provide it with her PII.

95. Ms. Charley provided IWP with her PII in order to purchase and receive prescription deliveries from IWP. Ms. Charley would not have provided her PII to IWP had she known that IWP would not protect it as promised.

96. In February 2022, Ms. Charley became aware that her PII was impacted by the Data Breach. Ms. Charley called IWP's call center to confirm her information was stolen. However, IWP's representatives would not provide Ms. Charley with specific details of what type of information was accessed by the unauthorized actor(s).

97. As a result of the Data Breach, Ms. Charley expends considerable time and effort monitoring her accounts to protect herself from additional identity theft. Ms. Charley fears for her personal financial security and is experiencing feelings 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 the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

98. Ms. Charley stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

99. Ms. Charley suffered actual injury in the form of damages to and diminution in the value of her PII --a form of intangible property that Ms. Charley entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

100. Ms. Charley has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

101. Both Plaintiffs remain at a continued risk of harm due to the exposure and potential misuse of their personal data by criminal hackers.

CLASS ACTION ALLEGATIONS

102. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and all members of the proposed Class ("Class"), defined as follows:

> All individuals residing in the United States whose personal information was compromised in the Data Breach disclosed by Injured Workers Pharmacy in February 2022.

103. 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 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.

104. Plaintiffs reserve the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

105. Plaintiffs and members of the Class satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The exact number of the members of the Class is unknown but, upon information and belief, the number exceeds 75,700, and individual joinder in this case is impracticable. Members of the Class 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.

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

c. **Adequacy**. Plaintiffs will fairly and adequately represent and protect the interests of the Class and have 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 Plaintiffs.

d. **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:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and members of the Class's PII;

ii. Whether Defendant breached the duty to use reasonable care to safeguard Plaintiffs' and members of the Class's PII;

iii. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Class's PII;

iv. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

v. 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 members of the Class's PII from unauthorized release and disclosure;

vi. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

vii. Whether Defendant's delay in informing Plaintiffs and members of the Class of the Data Breach was unreasonable;

viii. Whether Defendant's method of informing Plaintiffs and other members of the Class of the Data Breach was unreasonable;

ix. Whether Defendant's conduct was likely to deceive the public;

x. Whether Defendant is liable for negligence or gross negligence;

xi. Whether Plaintiffs and members of the Class were injured as a proximate cause or result of the Data Breach;

xii. Whether Plaintiffs and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiffs and members of the Class.

xiii. Whether Defendant's practices and representations related to the Data Breach breached implied warranties.

xiv. What the proper measure of damages is; and

xv. Whether Plaintiffs and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

e. **Superiority:** A class action is also a fair and efficient method of adjudicating the controversy 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.

106. 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 procedural device;

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

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

107. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

108. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

109. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII when it was no longer required to retain pursuant to regulations, including that of former patients.

110. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing

access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who made that happen.

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

112. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

113. Defendant owed these duties to Plaintiffs and members of the Class 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 members of the Class's PII for pharmaceutical services. Plaintiffs and members of the Class needed to provide their PII to Defendant to receive pharmaceutical services from Defendant, and Defendant retained that information.

114. The risk that unauthorized persons would try to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would try to access Defendant's databases containing the PII—whether by malware or otherwise.

115. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Class and the importance of exercising reasonable care in handling it.

116. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injuries.

117. Defendant also breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and members of the Class's injuries-in-fact.

118. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiffs, and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

119. But- for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and members of the Class, the PII of Plaintiffs and members of the Class would not have been compromised.

120. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and members of the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and members of the Class was compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

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

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

122. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

123. Defendant had a duty to protect and maintain and provide adequate data security to maintain Plaintiffs and the Class's PII under § 5 of the FTC Act, 15 U.S.C. § 45.

124. The FTC Act prohibits unfair business practices affecting commerce, which the FTC has interpreted to include a failure to use reasonable measures to safeguard PII.

125. Defendant's violation of these duties is negligence *per se* under Massachusetts law.

126. Plaintiffs and the proposed Class are included in the class of persons that the FTC Act was intended to protect.

127. The harm the Data Breach caused is the type the FTC Act was intended to guard against.

128. Defendant's negligence *per se* caused Plaintiffs and the proposed Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and

money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

129. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

130. Defendant offered to provide goods and services to Plaintiffs and members of the Class in exchange for payment.

131. To receive services, Defendant also required Plaintiffs and the members of the Class to provide Defendant with their PII, including their names and Social Security numbers.

132. In turn, Defendant agreed it would not disclose the PII it collects from patients to unauthorized persons. Defendant also impliedly promised to maintain safeguards to protect its patients' PII.

133. Defendant recognized its implied promise in its Breach Notice, stating that "safeguarding the privacy of information held in [its] care and the security of [its] network are among IWP's highest priorities." Exh. A.

134. Plaintiffs and members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for receiving Defendant's goods and services and then by paying for and receiving the same.

135. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access or theft of their PII.

136. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant without such agreement with Defendant.

137. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its e-mail systems that compromised such information. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

138. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

139. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

140. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

141. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

142. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

143. In these and other ways, Defendant violated its duty of good faith and fair dealing.

144. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

145. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

146. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

147. Plaintiffs and members of the Class conferred a monetary benefit upon Defendant in the form of monies paid for pharmaceutical services.

148. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs' and members of the Class's PII, as this was used to facilitate payment and pharmaceutical services.

149. As a result of Defendant's conduct, Plaintiffs and members of the Class suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and members of the Class paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

150. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiffs and members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

151. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

152. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

153. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

154. Defendant owed a duty to its patients, including Plaintiffs and the Class, to keep this information confidential.

155. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

156. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant to receive pharmaceutical services, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in

their belief that such information would be kept private and would not be disclosed without their authorization.

157. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

158. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

159. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

160. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

161. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

162. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

163. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

164. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which

includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CLAIM FOR RELIEF

Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

165. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 151 as if fully set forth herein.

166. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its patients, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

167. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure the PII of its patients.

168. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to adequately protect against cybersecurity events and give notice of the Data Breach in a reasonable and practicable period of time.

169. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the IT systems containing Plaintiff's and Class Members' PII.

170. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

171. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

172. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

173. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

174. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

175. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

176. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

177. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

178. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

179. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

180. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

181. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

182. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from

identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

183. As a direct and proximate result of Defendant's breaching its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

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

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

Dated: May 24, 2022.

By: 

H. Luke Mitcheson
MORGAN & MORGAN
1601 Trapelo Road, Suite 1601
Boston, MA 02110
Telephone: (857) 383-4905
Facsimile: (857) 383-4930)
lmitcheson@forthepeople.com

Samuel J. Strauss*
Raina C. Borrelli*
Alex Phillips*
TURKE & STRAUSS LLP
sam@turkestrauss.com
raina@turkestrauss.com
alexp@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Jean S. Martin*
Francesca Kester*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Gary M. Klinger*
Milberg Coleman Bryson Phillips Grossman, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

**Pro hac vice application forthcoming*

Counsel for Plaintiffs and the Proposed Class

ClassAction.org
