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

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

ALEXSIS WEBB and MARSCLETTE CHARLEY, on behalf of themselves and all others similarly situated

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

MORGAN & MORGAN, 1601 Trapelo Road, Suite 1601
Boston, MA 02110, Telephone: (857) 383-4905

DEFENDANTS

INJURED WORKERS PHARMACY, LLC

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Negligence, Negligence Per Se, Breach of Implied Contract, Unjust Enrichment, Invasion of Privacy, Breach of Fiduciary Duty

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5000000

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 05/24/2022

SIGNATURE OF ATTORNEY OF RECORD /s/ H. Luke Mitcheson

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach) - CA records only>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Injured Workers Pharmacy ("IWP") writes to notify you of a recent event that may affect the security of some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and what you may do to better protect your personal information, should you feel it appropriate to do so.

What Happened? On or about May 11, 2021, IWP learned of suspicious activity related to an IWP employee email account. In response, we launched an investigation to assess the security of our systems and to confirm the full nature and scope of the activity. This investigation revealed that an unknown actor accessed a total of seven (7) IWP e-mail accounts between January 16, 2021 and May 12, 2021. Accordingly, IWP, with the assistance of data review specialists, undertook a comprehensive and time-intensive review of the contents of the affected email accounts to determine if they contained personal information and, if so, to whom the information related. This review determined that the affected e-mail accounts contained patient information in IWP systems.

What Information was Involved? While we currently have no evidence that any information has been misused, the investigation determined the following types of your information were contained in an affected email account: your <<b2b_text_2(name, data elements)>><<b2b_text_4(name, data elements cont)>>.

What We Are Doing. Safeguarding the privacy of information held in our care and the security of our network are among IWP's highest priorities. Upon learning of this event, we immediately reset passwords to impacted accounts, and investigated and remediated the event. We also took action to further enhance our security measures already in place to protect our email systems and data. IWP also reported this event to government regulators.

What You Can Do. IWP encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Your Personal Information* for useful information on what you can do to better protect against possible misuse of your information.

For More Information. If you have additional questions, you may our call center at (855) 545-2591 (toll free), Monday through Friday, 9:00 am to 6:30 pm Eastern Time, excluding U.S. holidays. You may also write to IWP at 300 Federal Street, Andover, MA 01810.

We sincerely regret any inconvenience or concern this may have caused you. IWP remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Michael Gavin
President and CEO
Injured Workers Pharmacy

Steps You Can Take to Help Protect Your Personal Information

Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. IWP is located at 300 Federal Street, Andover, MA 01810.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are 503 known Rhode Island residents impacted by this event.

Exhibit B

Injured Workers Pharmacy Privacy Statement

Effective Date: July 14, 2021

Injured Worker's Pharmacy LLC ("IWP," "we," or "us") respects your concerns about privacy. This Privacy Policy describes how IWP may collect Personally Identifiable Information (PII) about you through your interactions with us at our Pharmacy, on our website, or when you otherwise communicate with us (collectively, our "Services"). This Privacy Policy also describes how we may use and disclose your PII, the choices available to you regarding our use of the information, and the measures we take to protect the security of the information. By using our Services, you agree to the terms of this Privacy Policy.

Updates to the Privacy Policy

We reserve the right to change this Privacy Policy without prior notice to you. The "Effective Date" noted above reflects the last time revisions were made to this Privacy Policy. Any changes will become effective at the time of posting and your use of our Services following these changes means that you accept the revised Privacy Policy.

PII We Obtain

PII is any information that we can use to identify, locate, or contact you. We may collect and store your PII when you provide it to us via our Services. Some examples of PII we collect and when we collect it include:

- contact information, such as name, phone number, postal address, and email address;
- demographic information, such as date of birth and gender;
- when you request that prescriptions be sent to you, we store billing and shipping information as a convenience to you for future purchases, and we will store information about your orders for order tracking and status retrieval purposes;
- when you enroll in our services via our website;
- when you indicate that you are interested in receiving information about our Services, such as e-mail alerts or other notifications.

If you choose not to provide your PII to us, we may not be able to provide you with requested products, services, or information.

If you submit any PII relating to other people in connection with our Services, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

Use and Disclosure of PII

IWP uses your PII to respond to your requests, including to fulfill your order, to improve reorder experiences, to communicate with you about your account, and to provide you with related customer service. We may also use your information to send marketing communications and administrative information to you.

We may use your PII for our business purposes. Internal use may include data analysis, audits, fraud monitoring and prevention, developing our services and determining the effectiveness of our promotional campaigns, and operating and expanding our business activities. This information may also be disclosed to our service providers in relation to services such as website hosting, data analysis, payment processing, order fulfillment, information technology, and related infrastructure provision, customer service, email delivery, auditing, and other services.

We may also transfer or share your PII to the extent we engage in business negotiations with third parties or in the event that some or all of our business, assets, or stock are sold or transferred (including in connection with any bankruptcy or similar proceedings) or used as security.

If requested, we may also provide your PII to law enforcement officials or judicial authorities. In matters involving claims of personal or public safety or in litigation where the information is pertinent (including to allow us to pursue available remedies or limit the damages that we may sustain), we may use or disclose PII, including without court process. We may also use or disclose PII to enforce our terms and conditions, to protect our operations or those of any of our affiliates, or to protect our rights, privacy, safety, or property and/or that of our affiliates, you, or others.

We may use and disclose PII to investigate security breaches or otherwise cooperate with authorities pursuant to a legal matter.

We may use and disclose information that does not personally identify you (including the information noted below in “Cookies and Information We Automatically Collect”) for any purpose, except to the extent limited by applicable law. If we are required to treat such information as PII under applicable law, then we may use it for all the purposes for which we use and disclose PII. We may also combine information that does not personally identify you with PII. If we do, we will treat the combined information as PII as long as it is combined.

Security of PII

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. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account with us has been compromised), please immediately contact us in accordance with the “How to Contact Us” section below.

You are responsible for maintaining the confidentiality of the credentials you utilize to access our Services and for restricting access to your device, and you agree to accept responsibility for all activities that occur in association with your credentials.

Telephone, Text, and Fax Policy

By providing your residential, wireless, business phone, and/or fax number(s) to IWP, you expressly consent to receive marketing and non-marketing autodialed and/or pre-recorded calls, text messages, and faxes (including

fax advertisements) from or on behalf of us at the number(s) provided. Your consent to receive calls, texts, or faxes is not a condition of the use of our Services and your consent may be revoked at any time by calling the toll-free number at **(888) 295-3989** or faxing your opt-out request to **(626) 608-2599**. You may also send an opt-out request via email to privacy@IWPharmacy.com with the phone and/or fax number you wish to opt out of. Your wireless carrier's standard message and data rates may apply.

Cookies and Information We Automatically Collect

When you interact with our Services, we obtain certain information by automated means, such as cookies, web server logs, web beacons, and other technologies. A “cookie” is a text file that websites send to a visitor’s computer or other Internet-connected devices to uniquely identify the visitor’s browser or to store information or settings in the browser. A “web beacon,” also known as an Internet tag, pixel tag, or clear GIF, links web pages to web servers and their cookies and may be used to transmit information collected through cookies back to a web server.

We may use cookies and other automated technologies to collect information about your equipment, browsing actions, and usage patterns. The information we obtain in this manner may include your device IP address, identifiers associated with your devices, types of devices connected to our services, web browser characteristics, device characteristics, language preferences, referring/exit pages, clickstream data, and dates and times of website visits. These technologies help us (1) remember your information so you will not have to re-enter it; (2) track and understand how you use and interact with our products and services; (3) tailor our Services around your preferences; (4) measure the usability of our Services and the effectiveness of our communications; (5) provide customer support; and (6) otherwise manage and enhance our Services.

Your browser may tell you how to be notified when you receive certain types of cookies or how to restrict or disable certain types of cookies. You can also find out how to do this for your browser by clicking “help” on your browser’s menu or by visiting www.allaboutcookies.org. For mobile devices, you can manage how your device and browser share certain device data by adjusting the privacy and security settings on your device.

Third-Party Web Analytics

We use third-party web analytics services, such as Google Analytics and HubSpot Analytics, on our website. The service providers that administer these services use automated technologies to collect data (such as IP addresses, cookies, and other device identifiers) to evaluate the use of our Sites.

Online Tracking and Internet-Based Advertising

Through our Services, we may collect information about your online activities. You may see advertisements for our Services on other websites or mobile apps because we engage in online advertising. This allows us to target our messaging to users. Advertisement technology companies track users’ online activities over time by collecting information through automated means, including through the use of cookies, web server logs, web beacons, and other similar technologies. This information is used to show advertisements that may be tailored to individuals’ interests, to track users’ browsers or devices across multiple websites, and to build a profile of users’ online browsing activities. The information collected may include data about users’ visits to websites that participate in the online ad ecosystem, such as the pages or advertisements viewed, and the actions taken on the websites. This data collection takes place both on our website and on third-party websites that participate in the online advertisement ecosystem. This process also helps us track the effectiveness of our marketing efforts.

To learn how to opt-out of interest-based advertising, please visit www.aboutads.info/choices and www.networkadvertising.org/choices/.

Your Choices and Access

You can remove yourself from our distribution lists at any time by contacting compliance@iwpharmacy.com. If you opt-out of receiving promotional emails from us, we may still send you important administrative messages, from which you cannot opt out.

You can request the removal or modification of the PII you have provided to us by utilizing the Contact Us section of our website, emailing us at privacy@IWPharmacy.com, calling us toll-free at **(888) 295-3989**, or faxing us at **(626) 608-2599**. For your protection, we may only implement requests with respect to the PII associated with the email address that you use to send us your request, and we may need to verify your identity and obtain information on the context in which you provided your PII before implementing your request. We will try to accommodate your request as soon as reasonably practicable.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting such change or deletion. There may also be residual information that will remain within our databases and other records, which will not be removed.

If you are a California consumer, for more information about your privacy rights, please see our California Consumer Privacy Rights page.

For any questions about this Privacy Statement, please contact IWP by telephone, email, or postal mail.

IWP PO Box 338
Methuen, MA 01844
Toll free: 1-888-321-7945
Fax: 1-800-305-0499

Customer Service is available from 8:00am to 8:00pm EST, Monday to Friday and 8:00am to 12:00pm EST on Saturday

Toll Free: 1-888-321-7945
Prescription Fax Hotline: 800-497-4276
Address: PO Box 338 Methuen, MA 01844

REFUND POLICY

By law, we cannot accept returns of prescription products for reuse or resale. However, if you feel we have made an error in filling the prescription, please call Customer Service toll-free, at 1-888-321-7945 with details of the error.

We will request special authorization for a return of the prescription.

ACHC ACCREDITED

LegitScript IWPHARMACY.COM 05/10/22 Certified

CONNECT WITH US

✎AO 440 (Rev. 10/93) Summons in a Civil Action

UNITED STATES DISTRICT COURT

District of **Massachusetts**

ALEXSIS WEBB and MARSCLETTE CHARLEY,

V.

INJURED WORKERS PHARMACY, LLC,

SUMMONS IN A CIVIL CASE

CASE

TO: (Name and address of Defendant)

INJURED WORKERS PHARMACY, LLC,
c/o Resident Agent:
C T CORPORATION SYSTEM
155 FEDERAL ST., STE. 500
BOSTON, MA 02110 USA

YOU ARE HEREBY SUMMONED and required to serve upon PLAINTIFF'S ATTORNEY (name and address)

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

an answer to the complaint which is herewith served upon you, within **20** days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint. You must also file your answer with the Clerk of this Court within a reasonable period of time after service.

CLERK

DATE

(By) DEPUTY CLERK

✎AO 440 (Rev. 10/93) Summons in a Civil Action

RETURN OF SERVICE

Service of the Summons and complaint was made by me(1)	DATE
NAME OF SERVER *(PRINT)*	TITLE

Check one box below to indicate appropriate method of service

G Served personally upon the third-party defendant. Place where served: _____

G Left copies thereof at the defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.

Name of person with whom the summons and complaint were left: _____

G Returned unexecuted: _____

G Other (specify): _____

STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on _____ _____
Date *Signature of Server*

_____
Address of Server

(1) As to who may serve a summons see Rule 4 of the Federal Rules of Civil Procedure.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

1. **Title of case (name of first party on each side only)** ALEXSIS WEBB v. INJURED WORKERS PHARMACY,LLC

2. **Category in which the case belongs based upon the numbered nature of suit code listed on the civil cover sheet. (See local rule 40.1(a)(1)).**

☐ **I.** **160, 400, 410, 441, 535, 830*, 835*, 850, 880, 891, 893, R.23, REGARDLESS OF NATURE OF SUIT.**

☐ **II.** **110, 130, 190, 196, 370, 375, 376, 440, 442, 443, 445, 446, 448, 470, 751, 820*, 840*, 895, 896, 899.**

☑ **III.** **120, 140, 150, 151, 152, 153, 195, 210, 220, 230, 240, 245, 290, 310, 315, 320, 330, 340, 345, 350, 355, 360, 362, 365, 367, 368, 371, 380, 385, 422, 423, 430, 450, 460, 462, 463, 465, 480, 485, 490, 510, 530, 540, 550, 555, 560, 625, 690, 710, 720, 740, 790, 791, 861-865, 870, 871, 890, 950.**

***Also complete AO 120 or AO 121. for patent, trademark or copyright cases.**

3. **Title and number, if any, of related cases. (See local rule 40.1(g)). If more than one prior related case has been filed in this district please indicate the title and number of the first filed case in this court.**

4. **Has a prior action between the same parties and based on the same claim ever been filed in this court?**

YES ☐ **NO** ☑

5. **Does the complaint in this case question the constitutionality of an act of congress affecting the public interest? (See 28 USC §2403)**

YES ☐ **NO** ☑

If so, is the U.S.A. or an officer, agent or employee of the U.S. a party?

YES ☐ **NO** ☐

6. **Is this case required to be heard and determined by a district court of three judges pursuant to title 28 USC §2284?**

YES ☐ **NO** ☑

7. **Do all of the parties in this action, excluding governmental agencies of the United States and the Commonwealth of Massachusetts ("governmental agencies"), residing in Massachusetts reside in the same division? - (See Local Rule 40.1(d)).**

YES ☐ **NO** ☑

A. **If yes, in which division do all of the non-governmental parties reside?**

Eastern Division ☐ **Central Division** ☐ **Western Division** ☐

B. **If no, in which division do the majority of the plaintiffs or the only parties, excluding governmental agencies, residing in Massachusetts reside?**

Eastern Division ☑ **Central Division** ☐ **Western Division** ☐

8. **If filing a Notice of Removal - are there any motions pending in the state court requiring the attention of this Court? (If yes, submit a separate sheet identifying the motions)**

YES ☐ **NO** ☐

(PLEASE TYPE OR PRINT)

ATTORNEY'S NAME H. Luke Mitcheson

ADDRESS 1601 Trapelo Road, Suite 1601, Boston, MA 02110

TELEPHONE NO. (857) 383-4905