UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA
OMAHA DIVISION

MARINA MAULDIN, individually and on behalf all other similarly situated,

Plaintiff,

v.

WEST TECHNOLOGY GROUP, LLC,

Defendant.

Case No.:

Judge:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Marina Mauldin ("Plaintiff") bring this Class Action Complaint against West Technology Group, LLC ("West Technology," or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant West Technology Group, LLC, formerly dba as Intrado Corporation, a private global technology company that provides cloud-based and data related services to its clients around the world.[1] Although Defendant is a technologically sophisticated entity, it failed to implement and maintain reasonable data security measures. As a result of Defendant's failures, sensitive personal information belonging to Plaintiff and Class Members was compromised in the course of a Data Breach. Plaintiff seeks damages on behalf of herself and Class Members, as well as equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiff and Class Members.

[1] About us, West.com, https://www.west.com/about-us (last visited Apr. 26, 2023).

2. Before and through December 2022, Defendant obtained Plaintiff's and Class Members' personally identifiable information ("PII") and stored that PII in an Internet-accessible environment on Defendant's network.

3. On or between November 25, 2022, and December 1, 2022, West Technology's network was breached in a cyberattack targeting the valuable personal information it contained (the "Data Breach").[2] Defendant discovered this attack after the fact and began investigating it in early December 2022. Three months later, in March 2023, Defendant was finally able to determine what information was involved in the Data Breach and to whom it belonged. On April 17, 20233, Defendant sent notice letters out to those individuals who were directly impacted by the cyberattack, notifying them of the Breach and their potential exposure.[3]

4. The Data Breach Notice Letter stated the following:

> WHAT HAPPENED? On December 1, 2022, we detected that an unauthorized third party gained remote access to WEST TECHNOLOGY's corporate network. We quickly took steps to secure our network and began an investigation of the incident with the support of leading outside cybersecurity experts as well as notified law enforcement.
>
> WHAT INFORMATION WAS INVOLVED? Our investigation to date has revealed that the unauthorized party took some files from WEST TECHNOLOGY's corporate network, which may have included certain employee personal information. We reviewed the files that may have been taken and on March 22, 2023, unfortunately, we determined your personal information was included in the potentially taken files.[4]

5. The specific data exposed—and then stolen—was a variety of PII. Specifically, Defendant lost names, dates of birth, Social Security numbers, driver's license or state

---

[2] *Office of the Main Attorney General, Data Breach Notifications* https://apps.web.maine.gov/online/aeviewer/ME/40/b463aadb-2070-4c90-bc34-ab641baa884a.shtml (last accessed April 26, 2023)

[3] PDF link accessible at: *Office of the Main Attorney General, Data Breach Notifications* https://apps.web.maine.gov/online/aeviewer/ME/40/b463aadb-2070-4c90-bc34-ab641baa884a.shtml (last accessed April 26, 2023)

[4] *Id*.

identification numbers, passport numbers, medical information, health insurance information, and/or financial account information.[5]

6. According to West Technology's posted cyber security update on its website, as well as the Notice Letter it sent Attorneys General and some Class Members, West Technology Group "detected that an unauthorized third party gained remote access to West Technology Group's corporate network," before taking steps to try to secure its network and investigate the cause and scope of the Data Breach "with the support of leading outside cybersecurity experts."[6]

7. The posted notice on Defendant's website further states that Defendant "encourage[s] affected current and former employees to take advantage of the free credit monitoring and identity theft protection services that we are providing to eligible individuals. In addition, affected individuals should remain vigilant and carefully review accounts for any suspicious activity."[7]

8. Plaintiff brings this action on behalf of all persons whose PII was compromised due to West Technology's failure to: (i) adequately protect Plaintiff's and Class Members' PII; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively monitor West Technology Group's network for security vulnerabilities and incidents. West Technology's conduct amounts at least to negligence and violates federal and state statutes.

9. Plaintiff and Class Members have suffered injuries due to West Technology Group's conduct. These injuries include: (i) lost or diminished value of PII; (ii) loss of privacy (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with

[5] https://www.west.com/security-incident (last accessed April 26, 2023)
[6] *Id.*
[7] *Id*.

attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (v) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (vi) charges and fees associated with fraudulent charges on their accounts, and (vii) the present, continued, and certainly an increased risk to their PII, which remains in West Technology's possession and is subject to further unauthorized disclosures so long as West Technology fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

10. West Technology Group disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently, failing to take and implement adequate and reasonable measures to ensure that Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, Plaintiff's and Class Members' PII was compromised through disclosure to unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

11. Plaintiff Marina Mauldin is a citizen of Texas residing in Grayson County, Texas, where she has lived at all times relevant and material to this action, and where she intends to continue to live for the foreseeable future.

12. Defendant West Technology Group, LLC is a limited liability company headquartered in Omaha, Nebraska. West Technology is incorporated under the laws of Delaware. Defendant's principal place of business is located at 11650 Miracle Hills Drive, 4th Floor, Omaha, NE 68154. Defendant can be served through its registered agent CSC-Lawyers Incorporating Service Company, 233 South 13th Street, Suite 1900, Lincoln, NE 68508. Defendant West Technology Group, LLC is owned and or managed by Olympus Holdings I, LLC, a limited liability company located at 11808 Miracle Hills Drive, 4th Floor, Omaha, NE 68154.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant, including that of Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

14. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Background

16. Defendant West Technology Group, LLC is a Nebraska based cloud and data services provider incorporated under the laws of Delaware.

17. In its Notice Letters sent to Class Members, posted online, and dispersed to notify the proper authorities, West Technology stated that "keeping personal data safe and secure is extremely important to us, and we deeply regret that this incident occurred."

18. Plaintiff and the Class Members, as current or former employees, reasonably relied (directly or indirectly) on this sophisticated data and information services corporation to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. People demand security to safeguard their PII, especially when Social Security numbers are involved as here.

19. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

Defendant Fails to Secure the PII, Resulting in a Data Breach

20. On or around April 17, 2023, West Technology first began notifying Class Members and state Attorneys General ("AGs") about a widespread breach of its computer systems and involving the sensitive personal identifiable information of Plaintiff and Class Members. Defendant explained that the Data Breach was detected on December 1, 2022.[8]

21. After detecting the Data Breach, Defendant "quickly took steps to secure our network and began an investigation of the incident with the support of leading outside cybersecurity experts." The "investigation" determined that Plaintiff's and Class Members' PII (possibly including names, dates of birth, Social Security numbers, driver's license or state identification numbers, passport numbers, medical information, health insurance information,

[8] *Id.*

and/or financial account information) may have been copied and acquired by unauthorized persons at the time of the incident. [9]

22. Defendant stated that it "deeply regret[s] that this incident occurred" in its apology and Notice to Plaintiff and Class Members.[10] Then, Defendant told the victims of the Data Breach to direct their concerns and questions to a call center—that is closed on weekends, and only open during select hours on weekdays.[11]

23. Upon information and belief, Plaintiff and Class Members in this action are current and former employees of West Technology Group, LLC.

24. According to the Notice posted on Defendant's website, the confidential information that was potentially accessed without authorization included at least names, dates of birth, Social Security numbers, driver's license or state identification numbers, passport numbers, medical information, health insurance information, and/or financial account information.

25. Upon information and belief, the PII was not encrypted prior to the data breach.

26. Upon information and belief, the cyberattack was targeted at West Technology as a large corporation that collects and maintains valuable personal, health, tax, and financial data.

27. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) Plaintiff's and Class Members' PII.

28. Defendant admitted in its Notice Letter that it only discovered the unauthorized access in early December, 2022, at which point that unauthorized access had been consistent for several days. The Notice does not communicate to Plaintiff or Class Members the reason for the

[9] *Id.*
[10] *Id.*
[11] *Id.*

delay in discovering the Data Breach, the reason for the three-month investigation, nor the reason for the additional month long delay in providing Notice to Plaintiff and Class Members.[12]

29. With its offer of credit and identity monitoring services to victims, Defendant is acknowledging that the impacted persons are subject to an imminent threat of identity theft and financial fraud as a result of its failure to protect the PII it collected and maintained.

30. In response to the Data Breach, Defendant fails to speak to the vulnerabilities in its cybersecurity systems and networks, and further fails to provide any assurances that steps will be made to better secure Plaintiff's and Class Members' PII going forward aside from "continu[ing] to work with leading cybersecurity experts…"[13]

31. West Technology had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep the PII that was entrusted to Defendant confidential, and to protect the PII from unauthorized access and disclosure.

32. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation that Defendant, as a sophisticated company directly plugged into the data and information sector, would comply with its duties, obligations, and representations to keep such information confidential and secure from unauthorized access.

33. West Technology failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

---

[12] *See Id.*
[13] *Id.*

35. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[14]

36. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, 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 email 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 least privilege in mind. If a user only needs to read specific files, the user should not have write 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.

[14] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Aug. 23, 2021).

- 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.[15]

37. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, 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

[15] *Id.* at 3-4.

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….[16]

38. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply 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 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 principle of least-privilege

- Monitor for adversarial activities

[16] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Aug. 23, 2021).

- 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].[17]

39. Given that Defendant was storing the PII of thousands of individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

40. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of thousands of individuals, including Plaintiff and Class Members.

Securing PII and Preventing Breaches

41. West Technology could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and computer files containing PII.

42. In its Notice Letter and online posted Notice, Defendant acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of Defendant's business purposes as a cloud and data services provider. Defendant acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that by

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Aug. 23, 2021).

law it may not disclose, and must take reasonable steps to protect, PII from improper release or disclosure.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

43. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

44. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[18]

45. In light of recent high profile data breaches, 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), West Technology Group, LLC knew or should have known that its electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

[18] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Oct. 11, 2022).

48. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

49. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[19]

50. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that **"*[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies.*** They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[20]

51. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that **"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening**

[19] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed Jan. 25, 2022).

[20] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed Jan. 25, 2022).

to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[21]

52. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

53. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of individuals in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

54. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

55. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

---

[21] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last accessed Jan. 25, 2022).

At All Relevant Times West Technology Group Had a Duty to Plaintiff and Class Members to Properly Secure their PII

56. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Defendant became aware that their PII may have been compromised.

57. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted West Technology with their PII as a condition of gaining employment at West Technology Group. Still others have entrusted sensitive data to Defendant as a condition of gaining access to Defendant's services.

58. West Technology had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

59. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

60. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[23]

61. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers as here, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of PII

62. Stolen personal information is one of the most valuable commodities on the information black market. According to Experian, a credit-monitoring service, stolen personal information can sell for over $1,000.00 (depending on the type of information).[24]

---

[22] 17 C.F.R. § 248.201 (2013).
[23] *Id.*
[24] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

63. The value of Plaintiff's and Class Members' personal information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites. Thus, after charging a substantial fee, criminals make such stolen information publicly available.

64. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[25] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[26]

65. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is likely readily available to others, and the rarity of the PII has been destroyed, thereby causing additional loss of value.

66. By failing to properly notify Plaintiff and the Class Members of the Data Breach, Defendant exacerbated their injuries. Specifically, by depriving them of the chance to take speedy measures to protect themselves and mitigate harm, Defendant allowed their injuries to fester and the damage to spread.

67. Social Security numbers, for example, 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

[25] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[26] *See* https://datacoup.com/ (last accessed Oct. 21, 2022).

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.[27]

68. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. 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.

69. Even then, a new Social Security number may not be effective, as "[t]he 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."[28]

70. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

---

[27] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 10, 2021).

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Dec. 10, 2021).

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 10, 2021).

71. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[30]

72. It can take years for victims to notice their identity was stolen—giving criminals plenty of time to sell one's personal information to the highest bidder.

73. One example of criminals using PII for profit is the development of "Fullz" packages.

74. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

75. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

76. That is exactly what is happening to Plaintiff and Class Members. And it is reasonable for any trier of fact, including this Court or a jury, to find that the stolen PII (of Plaintiff and the other Class Members) is being misused—and that such misuse is fairly traceable to Defendant's data breach.

[30] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

77. Over the past several years, data breaches have become alarmingly common. In 2016, the number of data breaches in the U.S. exceeded 1,000—a 40% increase from 2015.[31] The next year, that number increased further by nearly 45%.[32]

78. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets—so that they are aware of, and prepared for, a potential attack. One report explained that smaller entities "are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[33]

79. Thus, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry—including Defendant.

80. Responsible for handling highly sensitive personal information, Defendant knew or should have known the importance of safeguarding PII. Defendant also knew or should have known of the foreseeable consequences of a data breach. These consequences include the significant costs imposed on victims of the breach. Still, Defendant failed to take adequate measures to prevent the data breach.

81. Because of Defendant's inadequate practices, the PII of Plaintiff and the Class was exposed to criminals. In other words, Defendant opened up, disclosed, and then exposed its PII to

---

[31] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last accessed Aug. 15, 2022).

[32] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, IDENTITY THEFT RESOURCE CENTER (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last accessed Aug. 15, 2022).

[33] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed Aug. 15, 2022).

crooked operators and criminals. Such criminals engage in disruptive and unlawful business practices and tactics, like online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud)—all using stolen PII.

82. Given the nature of West Technology's Data Breach it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, simple credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[34] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

84. To date, Defendant has offered Plaintiff and Class Members only one year of credit monitoring services from their discovery of the Data Breach to the Notice Letters. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

85. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures to protect PII that it maintained.

---

[34] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Dec. 10, 2021).

West Technology Failed to Comply with FTC Guidelines

86. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[35]

87. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[36] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

88. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[37]

89. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

---

[35] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 10, 2021).

[36] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 10, 2021).

[37] FTC, *Start with Security*, *supra* note 59.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

90. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Because Class Members entrusted West Technology with their PII directly or indirectly, Defendant had, and has, a duty to the Class Members to keep their PII secure.

92. Plaintiff and the other Class Members reasonably expected that when they provided PII to Defendant that such PII would be protected and safeguarded.

93. Defendant was at all times fully aware of its obligation to protect the personal data of its customers and employees, including Plaintiff and members of the Classes. West Technology was also aware of the significant repercussions if it failed to do so.

94. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiff's and Class Members' full

names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed

95. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

96. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide Defendant with their sensitive personal information, Plaintiff and other Class Members reasonably understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received compensation that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

97. Cybercriminals target and capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff and the Class Members have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

98. The cybercriminals who targeted and obtained Plaintiff's and Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;

- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

99. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

100. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

101. Furthermore, certain PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[38]

102. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[39] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[40] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers

[38] *Id.*
[39] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (Feb. 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed Dec. 10, 2021).
[40] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed Dec. 10, 2021).

at a substantial risk of fraud."[41] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

103. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

Plaintiff Marina Mauldin's Experience

104. Plaintiff Marina Mauldin served as a Claims Adjuster for West Technology Group, LLC from February 27, 2018 through June 2020. As a condition of her employment, Plaintiff Mauldin was required to provide her sensitive private information to Defendant, including her name, date of birth, Social Security number, driver's license number, medical information, health insurance information, and financial account information.

105. Upon information and belief, at the time of the Data Breach—from November 25, 2022, to December 1, 2022— Defendant retained Plaintiff's PII in its system.

106. Plaintiff Mauldin is very careful about sharing her sensitive personal information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

107. Plaintiff Marina Mauldin received the Notice Letter, by U.S. mail, directly from Defendant, dated April 17, 2023. According to the Notice Letter, Plaintiff's PII was improperly

[41] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed Dec. 10, 2021).

accessed and obtained by unauthorized third parties, including her name and Social Security number, and possibly other valuable identifying information.

108. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including updating her passwords and resecuring her own computer systems. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. The time spent dealing with the repercussions of this Data Breach and attempting to mitigate its effects has been lost forever and cannot be recaptured.

109. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up 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 Private Information.

110. Plaintiff remains vigilant against instances of actual identity theft and fraud, and routinely checks all of her various accounts for fraudulent charges and suspicious activity. Since the Data Breach, Plaintiff has received a notable influx of spam calls, texts, and emails, some of which contain attempts to phish additional information from Plaintiff, and some of which contain disgusting and disturbing content and unsolicited advertisements.

111. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's cause and the reasons why Defendant retained her information after her employment ended. Further, the Plaintiff's anxiety and frustration are heightened by the fact that Defendant waited several months to disclose the Data Breach to Plaintiff and Class Members. The fear, anxiety, and distress are continuous in Plaintiff's life and are reinforced when Plaintiff is bombarded by spam and phishing emails, targeted advertisements, and intrusive thoughts about what specific information was compromised and in whose hands it is now.

112. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

113. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

114. Plaintiff Marina Mauldin has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

115. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

116. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around April 17, 2023 (the "Class").**

117. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

118. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

119. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are certainly tens of thousands, and possibly in excess of 100,000 individuals whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

120. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

d. Whether and when Defendant actually learned of the Data Breach;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

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

h. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

121. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

122. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members

uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

123. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

124. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

125. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm

the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

126. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

127. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

128. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

129. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

130. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

131. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

132. Plaintiff and the Class entrusted Defendant with their Private Information.

133. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

134. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

135. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

136. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession was adequately secured and protected.

137. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

138. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

139. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

140. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

141. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

142. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

143. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

144. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was stored on its database and was or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiff's and Class Members' Private Information.

145. Despite being aware of the likelihood that Defendant's databases were vulnerable, not secure, and likely to be attacked by cybercriminals, Defendant failed to correct, update, or upgrade its security protections, thus causing the Data Breach.

146. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

147. Defendant was in the best position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

148. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

149. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

150. Defendant has admitted that the Private Information of Plaintiff and Class Members was improperly accessed and exfiltrated by unauthorized third persons as a result of the Data Breach.

151. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

152. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

153. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

154. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

155. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it wase no longer required to retain pursuant to regulations.

156. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

157. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

158. Said differently, if Defendant had properly prevented a "technical security configuration," then the Data Breach would not have occurred, and Plaintiff's and Class Members' Private Information would have been appropriately safeguarded.

159. Plaintiff and Class Members suffered an injury when their Private Information was accessed by unknown third parties.

160. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, and increased risk of imminent harm, suffered by Plaintiff and the Nationwide Class.

161. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

162. As a direct and proximate result of Defendant's negligence, 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (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 Private Information, 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 Private Information in their 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.

163. As a direct and proximate result of Defendant' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

164. Additionally, as a direct and proximate result of Defendant's negligence Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in its continued possession.

165. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

166. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

167. Plaintiff and Class Members were required to provide Defendant with their Private Information.

168. By Plaintiff and Class Members providing their Private Information, and by Defendant accepting this Private Information, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiff's and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

169. Defendant provided consideration by providing employment in exchange for Plaintiff's and Class Members' PII, while Plaintiff and Class Members provided consideration by providing valuable property, their Private Information. Defendant benefitted from the receipt of

this Private Information by being able to utilize Plaintiff and Class Members' employment. In exchange for the Private Information, Defendant promised to protect their PII from unauthorized disclosure.

170. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

171. Defendant materially breached its implied contracts with Plaintiff and Class Members when it (1) placed their Private Information on a publicly available database that could (and later was) accessed by members of the public on the internet without a password or multi-factor authentication and (2) waited an unreasonably long time to notify them of the Data Breach. It is common sense that Plaintiff and Class Members would not have provided Defendant with their Private Information had they known that Defendant would not implement basic data security measures or that it would wait several months to notify them of a data breach involving their Private Information.

172. Defendant's breaches of contract have caused Plaintiff and Class Members to suffer damages from the lost benefit of their bargain, out of pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

173. As a direct and proximate result of Defendant's breaches of implied contract, 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (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 Private Information, 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 Private Information in their 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.

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

174. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

175. Plaintiff and Class Members are either current or former employees of West Technology Group.

176. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

177. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

178. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

179. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff and Class Members' Private Information.

180. 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.

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

182. As a direct and proximate result of Defendant's breaches 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (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 Private Information, 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 Private Information in their 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 breach of 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.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

184. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

185. Plaintiff and Class Members conferred a benefit on Defendant, by providing Defendant with their valuable Private Information, which was necessary for Defendant to receive the employment services of Plaintiff and Class Members.

186. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

187. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

188. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

189. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

190. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

191. Plaintiff and Class Members have no adequate remedy at law.

192. As a direct and proximate result of Defendant's actions, 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (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 Private Information, 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 Private Information in their 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.

193. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

194. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF

195. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

196. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

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

198. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

199. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

200. Defendant still possesses the Private Information of Plaintiff and the Class.

201. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

202. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

203. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at West Technology Group. The risk of another such breach is real, immediate, and substantial.

204. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

205. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

206. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at West Technology Group, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

207. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at West Technology Group, thus eliminating the additional injuries that would result to Plaintiff and Class.

208. Plaintiff and Class Members, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

209. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

210. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

211. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

212. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

213. Ordering that Defendant conduct regular database scanning and security checks; and

214. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

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

C. For injunctive relief requested by Plaintiff, including, but not limited to, orders requiring Defendant to enhance, update, upgrade, or otherwise improve hardware and software aspects of its cybersecurity arsenal, in addition to order compelling additional training, education, or preparation for Defendant's employees to better prepare them for further digital threats to Plaintiff's and Class Members' sensitive information;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 26, 2023

Respectfully Submitted,

/s/ *Gary M. Klinger*

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20016
Phone: 866.252.0878
dlietz@milberg.com

Terence R. Coates
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Attorney for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: West Technology Group Allegedly to Blame for December 2022 Data Breach

---