UNITED STATES DISTRICT COURT
THE DISTRICT COURT OF NEBRASKA

Fortuno Jeanfort, individually and on behalf of all others similarly situated, Plaintiff, v. TD Ameritrade, Inc., Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Fortuno Jeanfort ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through his counsel, files this Class Action Complaint against TD Ameritrade, Inc. ("TD Ameritrade" or "Defendant") and alleges the following based on personal knowledge of facts pertaining to himself and on information and belief based on the investigation of counsel as to all other matters.

INTRODUCTION

1. Between May 28, 2023 and May 30, 2023, an unknown actor gained access to TD Ameritrade's files that were saved on its MOVEit server. As a result, Plaintiff and the Class Members (as further defined below) have had their personal identifiable information ("PII")[1] exposed (the "Data Breach"). It is believed that the well-known Russian cybergang, CL0P ("Clop") is the source of the attack.[2]

[1] Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

2. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the PII of Plaintiff and Class Members. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

3. On or around May 30, 2023, Defendant claims they became aware that its MOVEit system had been breached.

4. According to Defendant, the PII exposed in the Data Breach includes names, Social Security numbers, financial account information, dates of birth, government identification numbers, and other personal identifiers.

5. Around August of 2023, Defendant began notifying Plaintiff and Class Members of the Data Breach.

6. Due to Defendant's negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

7. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the personal identifiable information of approximately 61,160 individuals[3] that was exposed in a major data breach of Defendant's files saved on the MOVEit server in violation of its legal obligations.

8. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Personal Information. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate,

[3] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/c680e116-4af9-489d-b74b-3715e373155e.shtml.

imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Personal Information, loss of privacy, and/or additional damages as described below.

9. Defendant betrayed the trust of Plaintiff and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

10. At this time, there exist many Class Members who are totally unaware their PII has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm.

11. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

12. Plaintiff brings this action, individually, and on behalf of all others whose PII was compromised as a result of Defendant's failure to adequately protect consumers' PII, timely discover the breach and warn its current and former customers of its inadequate information security practices, and effectively monitor its platforms for security vulnerabilities and incidents.

13. Plaintiff and Class Members have all suffered injury as a result of the Defendant's negligent conduct, including: (i) fraudulent credit card charges and identity theft. (ii) the potential for Plaintiff's and Class Members' exposed PII to be sold and distributed on the dark web, (iii) a lifetime risk of identity theft, sharing, and detrimental use of their sensitive information, (iv) out-

of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (vi) the continued and increased risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect its customers' PII.

14. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to equitable and injunctive relief.

I. THE PARTIES

15. Plaintiff Fortuno Jeanfort is a citizen of Boynton Beach, Florida.

16. Defendant TD Ameritrade, Inc. is incorporated in New York and headquartered in Omaha, NE. Defendant may be served by mailing a true and correct copy of the citation with this Complaint, including its attachments by U.S. certified mail, return requested, to C T Corporation System, 28 Liberty Street, New York, NY 10005.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

II. JURISDICTION AND VENUE

19. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA) and 28 U.S.C. § 1332(d) because this is a class action involving more than

100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class, including Plaintiff, are citizens of states different from Defendant.

20. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, and it regularly transacts business in this District.

21. Venue is proper in this district pursuant to 28 U.S.C. §1391(b)(2) because a substantial part of the events giving rise to the claim occurred in this District. Further, venue is proper in this district pursuant to 28 U.S.C. §1391(b)(2) because Defendant resides in Nebraska.

III. FACTUAL ALLEGATIONS

Background

22. TD Ameritrade provides investment advisory and brokerage services across the United States. In providing these services, Defendant requires the PII of Plaintiff and the Class Members.

23. Plaintiff and Class Members relied on this sophisticated Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Personal Information.

24. Defendant used the file transfer software MOVEit to move, store, and share files containing the Plaintiff and Class Members' PII.

25. Defendant had a duty to adopt reasonable measures to protect the Personal Information of Plaintiff and the Class Members from involuntary disclosure to third parties, including ensuring that all software sued to move, store, and/or share PII was secure.

Defendant's Data Breach

26. Between May 28, 2023 and May 30, 2023, due to Defendant's failure to maintain an adequate security system, an unknown hacker gained access to the Plaintiff and the Class's PII. This critical zero-day[4] flaw in the MOVEit software led to a wave of cyber-attacks against organizations who collected the sensitive PII of Plaintiff and the Class.[5] Multiple organizations have now confirmed data breaches, including the National Student Clearinghouse, PBI Research Services, TIAA, and Zellis.[6]

27. Defendant utilized the MOVEit software with complete disregard for its data security, infrastructure, procedures, and protocols.

28. Defendant knew of its duties to Plaintiff and the Class Members, and the risks associated with failing to protect the PII entrusted to it. Defendant knew that if it did not select a vendor with adequate security that Plaintiff's and the Class's PII would be unlawfully exposed.

29. Upon information and belief, Defendant failed to properly inquire about MOVEit data security before using it to store and transfer Plaintiff's and the Class's PII and failed to monitor and oversee its vendors data security. Had Defendant properly inquired about MOVEit's data security, overseen MOVEit's data security, and monitored MOVEit's data security, Plaintiff's and the Class's PII would have never been exposed in the Data Breach.

30. Defendant claim that it received notice of the Data Breach on May 30, 2023.

---

[4] "A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit." *See* https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability.

[5] *See* https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/.

[6] *Id.*

31. On or around August 2023, Defendant began sending Plaintiff and Class Members undated notices of the Data Breach ("Notice of the Data Breach").[7]

32. Defendant admitted in the Notice of the Data Breach that an unauthorized actor accessed sensitive personal information about Plaintiff and Class Members.

33. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

34. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

35. Defendant was negligent and did not use or implement reasonable security procedures, oversight and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

36. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

The Data Breach was Foreseeable

[7] *See* **Exhibit 1**

37. Preceding the Data Breach, Defendant knew or should have known that Defendant's MOVEit server was a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

38. 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."[8]

39. 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."[9]

40. 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 to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[10]

---

[8] 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 visited Aug. 17, 2023).

[9] 5 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 visited Aug. 17, 2023).

[10] 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 visited Aug. 17, 2023).

41. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant and Defendant's clients, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant and Defendant's clients, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

42. Considering the information readily available and accessible on the internet before the Data Breach and Defendant's involvement in data breach litigation, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members with a third-party without first ensuring that the third party's system was secure, Defendant had reason to know that Plaintiff and the Class Members PII was at risk for being shared with unknown and unauthorized persons.

43. Prior to 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.

44. Prior to the Data Breach, Defendant knew or should have known that it should have confirmed the information it obtained was encrypted within the PII to protect against their publication and misuse in the event of a cyberattack.

45. Prior to the Data Breach, Defendant knew or should have known that it should have confirmed that MOVEit's systems were secure and capable of protecting Plaintiff and the Class Members PII.

46. Since the breach, Defendant continues to store patient information, including Plaintiff's and Class Members' PII and has failed to give adequate assurances that it has enhanced its security practices sufficiently to avoid another breach of its servers in the future.

Defendant's Response to the Data Breach is Inadequate

47. Defendant was negligent and failed to inform Plaintiff and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

48. Defendant admitted that it learned of the data breach as early as May 30, 2023. Yet, Defendant did not start notifying affected individuals until almost a year later on or around mid-August 2023.

49. During these intervals, the cybercriminals have had the opportunity to exploit the Plaintiff and the Class Member's Personal Information while Defendant was secretly investigating the Data Breach.

Plaintiff's Experiences

50. Plaintiff received investment services from Defendant. In exchange, Defendant required Plaintiff's PII.

51. Defendant acquired, collected, and stored Plaintiff's PII and transferred it in the MOVEit Software.

52. Defendant was obligated by law, regulations, and guidelines to protect Plaintiff's and the Class's PII and Defendant was required to ensure that the MOVEit software had adequate data security, infrastructure, procedures, and protocols for Plaintiff's and the Class's PII.

53. Defendant was in possession of Plaintiff's PII before, during, and after the Data Breach.

54. Plaintiff received Defendant's Notice of Data Breach on August 3, 2023. The Notice stated that Plaintiff's PII was impacted by the Data Breach, including his name, Social Security number, financial account information, date of birth, government identification number, and other personal identifiers.

55. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor, including his name, Social Security number. Defendant has not yet provided definitive findings for Plaintiff to know. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

56. As a result of the Data Breach, Plaintiff had experienced fraudulent credit card use. His credit report has picked up unusual activity and unknown addresses.

57. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

58. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

59. Plaintiff stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

60. As a direct and traceable result of the Data Breach, Plaintiff suffered actual damages such as: (i) fraudulent credit card charges; (ii) lost time related to monitoring his accounts for fraudulent activity; (iii) loss of privacy due to his PII being exposed to cybercriminals; (iv) loss of the benefit of the bargain because Defendant did not adequately protect his PII; (v) severe emotional distress because identity thieves now possess his PII; (vi) exposure to increased and imminent risk of fraud and identity theft now that his PII has been exposed; (vii) the loss in value

of his PII due to his PII being in the hands of cybercriminals who can use it at their leisure; (viii) actual misuse of his PII; and (ix) other economic and non-economic harm.

61. Plaintiff has experienced actual misuse of his PII. After the breach, Plaintiff experienced a fraudulent credit card charges and unauthorized transactions on his credit report.

62. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

63. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

64. To his knowledge, Plaintiff has not been the victim of any other data breach.

Securing Personal Information and Preventing Breaches

65. Data breaches are preventable.[11] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[12] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[13]

66. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information

[11] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[12] *Id.* at 17.

[13] *Id.* at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[14]

67. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[15] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

68. Upon information and belief, Defendant failed to ensure that its vendors maintained reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendant also failed to ensure that its vendors met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical

[14] *Id.*

[15] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity preparation.

69. 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."[16]

70. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured its vendors 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.

[16] 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 visited July 17, 2023).

- 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.

- 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.[17]

71. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured its vendors 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

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

> a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
>
> - **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> - **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
>
> - **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> - **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[18]

72. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured its vendors 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 privilege credentials
>
> **Thoroughly investigate and remediate alerts**
> - Prioritize and treat commodity malware infections as potential full comprise

[18] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited July 17, 2023).

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

- 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].[19]

73. To prevent zero-day attacks, Defendant could and should have implemented, or ensured its vendors implemented, as recommended by Security Intelligence, the following:

- **Patch management:** Formal patch management can help security teams remain aware of critical patches.
- **Vulnerability management:** Vulnerability assessments and penetration tests can help companies detect zero-day vulnerabilities before adversaries find them.
- **Attack surface management (ASM):** ASM enables security teams to identify all network assets and scan them for vulnerabilities. ASM tools assess the network from an attacker's perspective, focusing on how threat actors might try to exploit assets.
- **Threat intelligence:** Security researchers are often the first to identify zero-day vulnerabilities. Organizations that receive threat intelligence updates may be informed about zero-day vulnerabilities sooner.
- **Anomaly-based detection methods:** Machine learning tools can spot suspicious activity in real-time. Common anomaly-based detection solutions include user and entity behavior analytics (UEBA), extended detection and response (XDR) platforms, endpoint detection and response

[19] *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 visited July 17, 2023).

(EDR) tools and some intrusion detection and intrusion prevention systems.[20]

74. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

75. Plaintiff and other Members of the Class entrusted their PII to Defendant.

76. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

77. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

78. Given that Defendant was storing the PII of other individuals, Defendant could and should have implemented all of the above measures, and ensured that the MOVEit Software did the same, to prevent and detect ransomware attacks.

79. 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 Plaintiff and Class Members.

80. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members, and ensuring the MOVEit software properly secured and encrypted the folders, files, and/or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have

[20] https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

81. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

82. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

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

The Value of PII

84. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 17, 2023).

[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July17, 2023).

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 17, 2023).

85. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

86. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[24]

87. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

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

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

90. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

[24] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 17, 2023).

information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

91. That is exactly what is happening to Plaintiff and members of the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

Plaintiff and the Class Face Significant Risk of Continued Identity Theft

92. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

93. Defendant negligently disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

94. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiff and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Personal Information in their possession.

95. The fraudulent activity resulting from the Data Breach may not come to light for years.

96. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

[25] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 17, 2023).

97. Defendant's negligence and failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach

98. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

99. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database and on Defendant's MOVEit server, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

100. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

101. To date, Defendant has offered Plaintiff and some Class Members two (2) years of identity monitoring services. 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 Personal Information at issue here.

102. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendant Failed to Adhere to FTC Guidelines

103. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PII.

104. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] 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."[27]

105. 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. The guidelines explain that businesses should:

a. Protect the sensitive consumer information that they keep;

b. Properly dispose of PII that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

[26] 17 C.F.R. § 248.201 (2013).
[27] *Id.*

106. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

107. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

108. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

109. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff and the Class's PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

IV. CLASS ACTION ALLEGATIONS

110. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Fed. R. Civ. P. 23 (b)(2), (b)(3), and (c)(4).

111. The Class that Plaintiff seeks to represent is defined as follows:

> **All individuals whose PII may have been accessed and/or acquired in the Data Breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and the Class Members on or around August 3, 2023.**

112. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. According to the Attorney General for the State of Maine Data Breach Notifications, the total number of persons affected by the Data Breach is 61,160.

113. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. All had their PII compromised as a result of the Data Breach.

114. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

115. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

116. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to ensure MOVEit was capable of adequately protecting their PII, and whether it breached this duty;

d. Whether Defendant breached its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Defendant failed to ensure MOVEit provided adequate cyber security;

f. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Defendant was negligent in utilizing MOVEit who permitted unencrypted PII off vast numbers of individuals to be stored within its network;

i. Whether Defendant was negligent in failing to ensure MOVEit adhered to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether Defendant breached implied contractual duties to Plaintiff and Class Members to use reasonable care in protecting their PII;

k. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

l. Whether Defendant continues to breach duties to Plaintiff and Class Members;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

118. While providing its services, Defendant gathered and stored the PII of Plaintiff and Class Members.

119. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no

ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between the Defendant and the Plaintiff and Class Members.

120. Defendant was well aware of the fact that cyber criminals routinely target corporations through cyberattacks in an attempt to steal the PII of employees, applicants, business associates, customers, and patients.

121. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and provide notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

122. Defendant had duties to protect and safeguard the PII of Plaintiff and Class Members from potential cyberattacks, including by ensuring Defendant and its vendors: (i) encrypted any document or report containing PII, (ii) did not permit documents containing unencrypted PII to be maintained on its systems, and (iii) took other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and Class Members include ensuring Defendant and its vendors:

a. Exercised reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. Protected the PII in its possession using reasonable and adequate security procedures and systems;

c. Adequately and properly audited and tested its systems;

d. Adequately and properly audited, tested, and trained its employees regarding how to properly and securely transmit and store PII;

e. Trained employees not to store PII for longer than absolutely necessary;

f. Implement processes to quickly detect a data breach, security incident, or intrusion; and

g. Promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

123. Plaintiff and Class Members were the intended beneficiaries of Defendant's duties, creating a special relationship between them. Defendant was in a position to ensure that MOVEit's systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it Defendant.

124. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to ensure MOVEit was capable of protecting the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to ensure the MOVEit software was adequately and properly audited and tested to avoid cyberattacks;

d. Failing to ensure Defendant and its vendors adequately and properly audit, test, and train their employees regarding how to properly and securely transmit and store PII, including maintaining PII in an encrypted format;

e. Failing to ensure Defendant and its vendors adequately and properly trained its employees not to store PII for longer than absolutely necessary;

f. Failing to ensure Defendant and its vendors consistently enforced security policies aimed at protecting Plaintiff and Class Members' PII;

g. Failing to ensure Defendant and its vendors implement processes to quickly detect data breaches, security incidents, or intrusions;

h. Failing to ensure Defendant and its vendors abided by reasonable retention and destruction policies for PII of former employees, applicants, business associates, customers, and patients; and

i. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII.

125. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

126. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

127. The damages Plaintiff and Class Members have suffered were and are reasonably foreseeable.

128. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

129. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

130. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

131. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which

occurred as a result of Defendant's failure to observe these duties, including the loss of privacy and significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

132. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII.

133. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders also form part of the basis of Defendant's duty in this regard.

134. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

135. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

136. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

137. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

138. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

139. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

140. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

141. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

142. Plaintiff and Class Member provided their PII to Defendant as a condition of their receipt of services.

143. When Plaintiff and Class Members provided their PII to Defendant as part of their receipt of services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their PII and to timely notify them in the event of a Data Breach.

144. Based on Defendant's legal obligations and acceptance of Plaintiff's and Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

145. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach.

146. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' PII.

147. Plaintiff and the Class have suffered injury, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

149. A relationship existed between Plaintiff and the Class Members and Defendant in which Plaintiff and the Class put their trust in Defendant to protect their PII. Defendant accepted this duty and obligation when it received Plaintiff and the Class Members' PII.

150. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and refrain from disclosing their PII to unauthorized third parties.

151. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII, including ensuring that its vendors used such care, involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal actions of a third party.

152. Defendant's fiduciary duty required it 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, ensuring and monitoring

its vendors' designing, maintaining, and testing of its security protocols to ensure that Plaintiff and the Class's information was adequately secured and protected.

153. Defendant also had a fiduciary duty to ensure that it and its vendors had procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's PII. 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 Defendant was entrusted with Plaintiff and the Class's PII.

154. Defendant breached its fiduciary duty that it owed Plaintiff and the Class by failing to act in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the PII of Plaintiff and the Class Members.

155. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiff and the Class.

156. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

157. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

158. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

159. When Plaintiff and Class Members provided their Personal Information to Defendant as a condition of receiving services, Plaintiff and proposed class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and proposed class members that their data had been breached and compromised.

160. Defendant solicited and invited Plaintiff and Class Members to provide their Personal Information as a condition of receiving services from Defendant.

161. Plaintiff and Class Members accepted Defendant's offer and provided their PII Defendant required, expecting that Defendant would exercise reasonable care to safeguard and maintain the confidentiality of their PII.

162. Each disclosure of PII was made pursuant to the mutually agreed upon implied contract with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify them that such information was compromised and breached.

163. Plaintiff and Class Members would not have provided and entrusted their PII in the absence of such implied contract between them and the Defendant.

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

165. Defendant breached their implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect Plaintiff's and Class Members' PII through the conduct detailed herein and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

166. The losses and damages sustained by Plaintiff and Class Members as described herein were the direct and proximate result of Defendant's breaches of the implied contracts between it and the Plaintiff and Class Members.

SIXTH CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

167. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

168. Plaintiff and Class Members have a reasonable expectation of privacy in their PII.

169. Defendant's negligent, reckless, and intentional conduct as alleged herein invaded Plaintiff's and Class Members' privacy.

170. By knowingly failing to keep Plaintiff's and Class Members' PII safe, and by knowingly misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant negligently, recklessly, and intentionally invaded Plaintiff's and Class Members' privacy by intruding into Plaintiff's and Class Members' private affairs, without approval, in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to a person of ordinary sensibilities.

171. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's negligent, reckless, and intentional actions highly offensive and objectionable.

172. Such an intrusion into Plaintiff's and Class Members' private affairs is likely to cause outrage, shame, and mental suffering because the Personal Information disclosed contained PII.

173. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private life by negligently, recklessly, and intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

174. The PII disclosed by Defendant has no legitimate reason to be known by the public.

175. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Personal Information without their informed, voluntary, affirmative, and clear consent.

176. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

177. In failing to protect Plaintiff's and Class Members' Personal Information, and in negligently, recklessly, and intentionally misusing and/or disclosing their Personal Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

SEVENTH CAUSE OF ACTION
BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Class)

178. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

179. As described above, when Plaintiff and Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with their statutory and common law duties and industry standards to protect Plaintiff's and Class Members' PII and timely detect and notify them in the event of a data breach.

180. Plaintiff and the Class Members were required to provide their PII to Defendant in exchange for services provided by Defendant. These exchanges constituted an agreement between the parties.

181. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have voluntarily disclosed their PII to Defendant but for the prospect of Defendant's promise of providing services. Conversely, Defendant presumably would not have received Plaintiff's and Class Members' PII if it did not intend to provide services to Plaintiff and the Class Members.

182. Implied in these exchanges was a promise by Defendant to ensure the Plaintiff's and Class Members' PII was only used to provide services from Defendant.

183. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their PII in exchange for Defendant's implied agreement to keep it safe and secure.

184. While Defendant had discretion in the specifics of how they met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

185. Defendant breached this implied covenant when they engaged in acts and/or omissions that are declared unfair trade practices by the FTC. These acts and omissions included: failing to protect Plaintiff's and Class members' PII, failing to ensure its vendors

possessed adequate cybersecurity protection, and failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

186. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do. All conditions required for Defendant's performance were met.

187. Defendant's acts or omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

188. Plaintiff and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have obtained their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

189. Defendant is liable for their breaches of these implied covenants, whether or not they are found to have breached any specific express contractual term.

190. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

EIGHTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

191. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

192. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable Personal Information.

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

194. 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.

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

196. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

198. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Personal Information is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) 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; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

fails to undertake appropriate and adequate measures to protect Personal Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

199. 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.

200. 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. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

Ninth Cause of Action
Injunctive and Declaratory Relief
(On Behalf of Plaintiff and the Class)

201. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

202. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

203. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that require it to adequately secure their PII.

204. Defendant still possess the PII of Plaintiff and the Class Members.

205. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class Members.

206. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

207. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate 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:

a. Ordering Defendant to ensure third-parties possessing its patients' PII engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

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

d. Ordering that Defendant guarantee third-parties possessing its patients' PII audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendant protect Plaintiff's and the Class's PII by, among other things, guaranteeing third-parties possessing its patients' PII have firewalls and

access controls so that if one area of the third-parties' systems are compromised, hackers cannot gain access to other portions of its systems;

f. Ordering that Defendant cease storing unencrypted PII on its systems;

g. Ordering that Defendant ensure that third-parties possessing its patients' PII conduct regular database scanning and securing checks;

h. Ordering Defendant to ensure third-parties possession its patients' PII routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

IV. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages,

attorneys' fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

I. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: August 28, 2023

Respectfully submitted,

/s/ Gary Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Applicants for Admission Pro Hac Vice:

William B. Federman
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081

COUNSEL FOR PLAINTIFF AND PROPOSED LEAD FOR THE PUTATIVE CLASS

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: TD Ameritrade Hit with Class Action Over Data Breach Affecting 61K
