IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DARLEEN LEWIS, *individually and on behalf of all others similarly situated*, Plaintiff, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	Case No. 2:24-cv-2258 JURY TRIAL DEMANDED

PLAINTIFF'S ORGINAL CLASS ACTION PETITION

Plaintiff Darleen Lewis ("Plaintiff") brings this Class Action Petition against Defendants Cencora, Inc. ("Cencora,") and The Lash Group, LLC ("Lash," or collectively "Defendants")[1], individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard protected health information ("PHI" or "Private Information") including, but not limited to, Plaintiff's and Class Members' names, addresses, dates of birth, health diagnosis and/or medications and prescriptions.

2. Defendants are an American drug wholesale company and a contract research organization. "Cencora connects manufacturers providers, pharmacies, and patients to help them seamlessly navigate the healthcare system from start to finish."[2]

[1] *We Are Cencora*, lashgroup.com.
[2] *What We Offer*, Cencora, https://www.cencora.com/what-we-offer (last visited May 27, 2024).

3. During the course of their business operations, Defendants acquired, collected, utilized, and derived a benefit from Plaintiff and Class Members' PHI. Therefore, Defendants owed and otherwise assumed statutory, regulatory, and common law duties and obligations, including to keep Plaintiff's and Class Members' Private Information confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach.

4. On or around February 21, 2024, Defendants "learned that data from their systems had been exfiltrated, some of which could contain personal information." After learning of the incident, Cencora launched an investigation to determine the nature and scope of the incident, and on April 10, 2024, confirmed Plaintiff's information was involved in the breach. [3]

5. As a result of Defendant's data security failure, an unauthorized third party was able to access and potentially obtain data containing Plaintiff and Class Members' PHI from their systems (the "Data Breach").[4]

6. Despite learning of the Data Breach on or about February 21, 2024, Defendants did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until May 17, 2024.

7. Based on the Notice of Data Breach Letter, Defendants admit that Plaintiff's and Class Members' Private Information was unlawfully accessed and may have been exfiltrated by a third party.

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' PHI that they collected and

[3] *More than 540,000 Patients Notified so far About Cencora/Lash Group Data Breach*, DataBreaches.net (May 24, 2024), Navvishealthcare.com, https://databreaches.net/2024/05/24/more-than-540000-patients-notified-so-far-about-cencora-lash-group-data-breach/.
[4] *Id.*

maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

9. Upon information and belief, Defendants maintained the PHI in a negligent manner. In particular, the PHI was maintained on computer systems and networks that were in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants; and, thus, Defendants was on notice that failing to take appropriate protective measures would expose and increase the risk that the PHI could be compromised and stolen.

10. Hackers can offer for sale the unencrypted, unredacted PHI to criminals. The exposed PHI of Plaintiff and Class Members can, and likely will, be sold repeatedly on the dark web, as is the *modus operandi* of cybercriminals.

11. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their PHI.

12. Plaintiff and Class Members reasonably expected Defendants to keep their PHI confidential and securely maintained, to use the information for business purposes only, and to make only authorized disclosures of this information.

13. Because of the Data Breach, Plaintiff and Class Members now face a current and ongoing risk of identity theft or fraud.

14. This PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PHI of Plaintiff and Class Members. In addition to Defendants' failure to prevent the Data Breach.[5]

15. As a result of this delayed response, Plaintiff and Class Members had no idea their PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

16. While many details of the Data Breach remain in the exclusive control of Defendants, upon information and belief, Defendants breached their duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendants' inadequate data security practices; (6) failing to encrypt or adequately encrypt the PHI; (7) failing to recognize or detect that their network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

17. As a result of Defendants' unreasonable and inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a)

[5] *Id.*

invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their PHI; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

18. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendant's data security systems, and future annual audits.

19. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct and asserting claims for: (i) negligence and (ii) unjust enrichment.

PARTIES

20. Plaintiff Darleen Lewis is a Citizen of Ohio residing in Butler County, Ohio. Plaintiff received a letter dated May 17, 2024, from Defendants notifying Plaintiff that Defendants' network had been accessed and Plaintiff's PHI was involved in the Data Breach.

21. Defendant Cencora, Inc., is a corporation organized under the laws of the state of Delaware, with a principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

22. Defendant The Lash Group, LLC is a limited liability company with its principal place of business located at 1 West 1st Avenue, Conshohocken, PA 19428.

JURISDICTION AND VENUE

23. 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 Defendants, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has personal jurisdiction over Defendants because they operate and are headquartered in this District and conduct substantial business in this District.

25. 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, Defendants are based in this District, maintain Plaintiff's and Class Members' PHI in this District, and have caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

The Data Breach

26. Cencora, Inc. is one of the leading global pharmaceutical sourcing and distribution services companies, that partners with pharmaceutical companies to "facilitate and optimize market access to therapies," and has more than 46,000 team members.[6]

27. In the ordinary course of their business, Defendants receive, store, maintain, and use Plaintiff and Class Members' Private Information, including but not limited to, their names, addresses, and medical treatment information.

[6] *Cencora, Inc. Form 8-K 2024*, Cencora, Inc. (May 1, 2024), https://investor.cencora.com/financials/sec-filings/default.aspx.

28. Given the sensitive nature of the PHI in their possession, Defendants knew, or should have known, the importance of securely storing and maintaining Private Information on their network.

29. On or about February 21, 2024, Defendants discovered their network had been breached by an unauthorized individual and learned that information from their network had been exfiltrated.

30. Following a forensic investigation, Defendants then discovered that unknown cybercriminals had accessed, obtained, and potentially exfiltrated the Private Information of Plaintiff and Class Members.

31. Defendants' Notice of Data Breach admits that Plaintiff's and Class Members' Private Information was accessed without authorization, and states that although it knew of the Data Breach as early as February 21, 2024, they waited until May 17, 2024 to begin mailing Notice to affected individuals.[7]

32. Defendants further admit that cybercriminals not only viewed and accessed Plaintiff's and Class Members' Private Information, but also acquired it from Defendants' network, meaning the Private Information was exfiltrated.[8]

Plaintiff Darleen Lewis's Experience

33. As a requisite to receiving medical services from healthcare from Defendants, Plaintiff provided her Private Information to Defendants and trusted that the information would be safeguarded according state and federal law. Upon receipt, Private Information was entered and stored on Defendants' network and systems.

[7] *Id.*
[8] *Id.*

34. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

35. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts. Had she known Defendants failed to follow basic industry security standards and failed to implement systems to protect her Private Information, she would not have provided that information to Defendant.

36. The Notice Letter dated May 17, 2024, from Defendants Cencora and Lash notified Plaintiff that their network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach, which included Plaintiff's names, dates of birth, address, and medical information.

37. Furthermore, Defendants directed Plaintiff to take certain steps to protect her Private Information such as enrolling in credit monitoring and carefully monitoring financial statements.

38. As a result of the Data Breach and Defendants' Notice of Data Breach, Plaintiff heeded Defendants' warning and spent more than two hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, and freezing her credit. This time has been lost forever and cannot be recaptured. Moreover, this time was spent, in part, at Defendants' direction by way of the Data Breach notice where Defendants advised Plaintiff to review her account statements.

39. Even with the best response, the harm caused to Plaintiff cannot be undone.

40. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

41. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

42. Plaintiff has suffered imminent and impending injury arising from the imminent and ongoing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

43. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

44. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

The Data Breach was Foreseeable

45. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendants' 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.

46. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, 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.

47. 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."[9]

48. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[10] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

50. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

51. 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 they

---

[9] *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).

[10] *See* 2021 Data Breach Annual Report, 6 (ITRC, Jan. 2022) available at https://notified.idtheftcenter.org/s/.

are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

52. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[12]

53. Therefore, 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.

Value of Private Information

54. The Private Information of consumers remains of high value to criminals, as evidenced by the prices offered 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.[13] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[14] Criminals can also purchase access to entire

[11] FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware.
[12] *See* Maria Hernandez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.
[13] *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/.
[14] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/

company data breaches from $900 to $4,500.[15]

55. 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.

56. 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…[is] worth more than 10x on the black market."[16]

57. 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.

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

59. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

60. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

61. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and

[15] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[16] 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 Aug. 23, 2021).

other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

62. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information 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.[17]

63. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the one year of protection offered by Defendant.

Defendants Failed to Properly Protect Plaintiff's and Class Members' Private Information

64. Defendants could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

65. Defendants' negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they possess.

---

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

66. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 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."[18]

68. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

69. To prevent and detect unauthorized cyber-attacks, Defendants 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

[18] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed May 1, 2023).

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.
- 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.[19]

70. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United

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

States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[20]

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

[20] *See* Security Tip (ST19-001) Protecting Against Ransomware (Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

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
- 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].[21]

72. Moreover, given that Defendants were storing the Private Information of Plaintiff and Class Members, Defendants could and should have implemented all of the above measures to

[21] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

prevent and detect cyberattacks.

73. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

74. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

75. Because Defendants failed to properly protect and safeguard Plaintiff and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system files and exfiltrate that data.

Defendants Failed to Comply with FTC Guidelines

76. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

77. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient 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 to correct any security

problems.[22]

78. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

79. The FTC further recommends that companies not maintain Private 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.

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

81. Upon information and belief, Defendants failed to properly implement basic data security practices.

82. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an

[22] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

83. Defendants were always fully aware of their obligation to protect the Private Information of Plaintiff and Class Members. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

84. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

85. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

86. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

87. Upon information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all

established standards in reasonable cybersecurity readiness.

88. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

89. Upon information and belief, Defendants failed to comply with one or more of the foregoing industry standards.

Defendants' Conduct Violates HIPAA and Evidences Its Insufficient Data Security

90. HIPAA requires covered entities and business associates of covered entities like Defendants to protect against reasonably anticipated threats to the security of sensitive patient health information.

91. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

92. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

93. A Data Breach such as the one Defendants experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI that is not permitted under HIPAA.

94. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or

disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

95. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[23]

96. Defendants' Data Breach resulted from a combination of insufficiencies that demonstrates Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants' Negligent Acts and Breaches

97. Defendants participated and controlled the development, implementation and enforcement of their privacy policy and controlled the process of gathering the Private Information from Plaintiff and Class Members.

98. Defendants therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendants breached these obligations to Plaintiff and Class Members and/or were otherwise negligent because they failed to properly implement data security systems and policies for its

[23] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

health providers network that would adequately safeguarded Plaintiff's and Class Members' Sensitive Information. Upon information and belief, Defendants' unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members Sensitive Information;

b. Failing to properly monitor their data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of their data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to put into develop and place uniform procedures and data security protections for their healthcare network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI their network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of their workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

p. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

q. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

r. Failing to implement or update antivirus and malware protection software in need of security updating;

s. Failing to require encryption or adequate encryption on their data systems;

t. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' Private Information provided to Defendants, which in turn allowed cyberthieves to access their IT systems.

COMMON INJURIES & DAMAGES

99. As result of Defendants' ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

100. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, potentially including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and

loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

101. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

102. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

103. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are

often the starting point for these additional targeted attacks on the victims.

104. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[24] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[25] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

105. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PHI at issue here.[26] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[27] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[28]

106. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health

---

[24] Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[25] *Id.*
[26] *What is the Dark Web?*, Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[27] *Id.*; Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[28] *What is the Dark Web?*, Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[29]

107. One such example of criminals using PHI for profit is the development of "Fullz" packages.

108. Cyber-criminals can cross-reference two sources of PHI 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.

109. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI 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. 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 Plaintiff's and Class Members' stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

110. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that

[29] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Sep. 13, 2022).

year, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

111. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[31] Defendants did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

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

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

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

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

[30] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Oct. 21, 2022).
[31] *Id.*

valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[32]

116. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[33]

117. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[34]

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

---

[32] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited May 28, 2015).

[33] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[34] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last accessed: October 21, 2022).

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

119. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

120. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice instructs them, "review[ing] health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred."

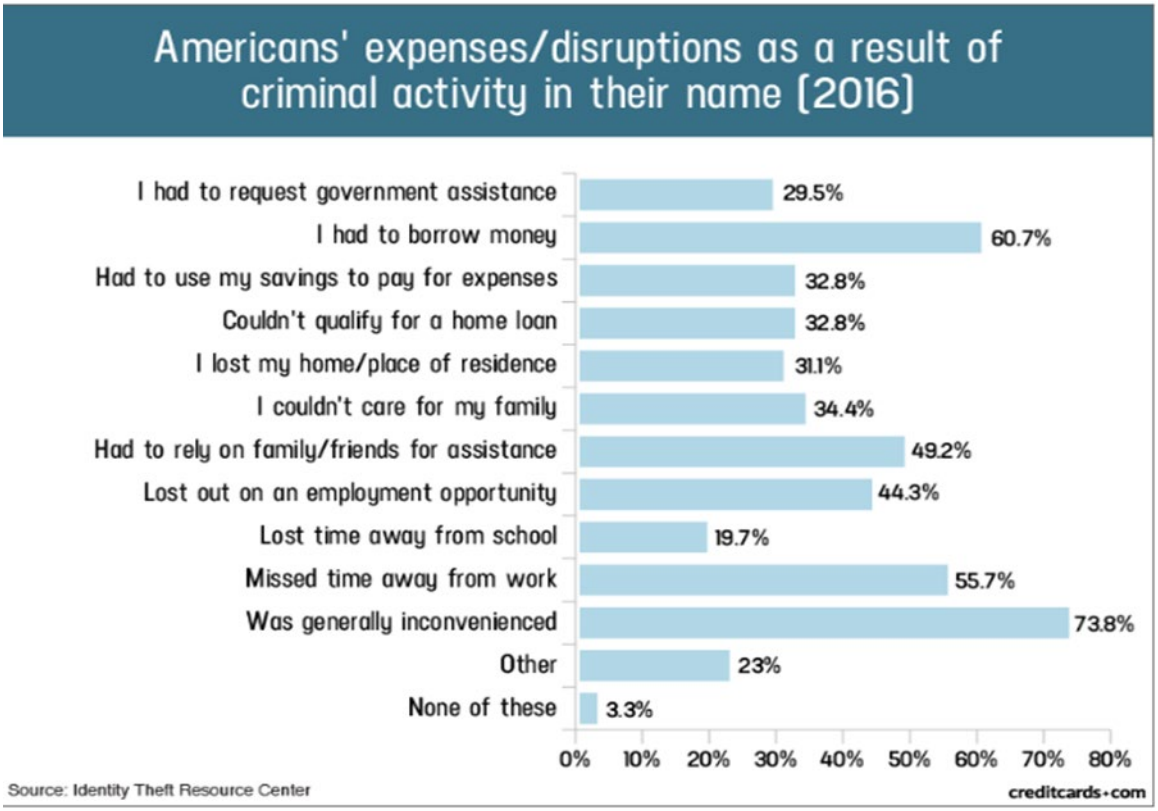
121. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

122. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[35]

[35] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

123. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[36]

124. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[37]



[36] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[37] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

125. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

Diminution of Value of the Private Information

126. PHI is a valuable property right.[40] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

127. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed

[38] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").
[39] *See* https://www.identitytheft.gov/Steps (last visited Sep. 13, 2022).
[40] *See*, *e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

PHI to adjust their insureds' medical insurance premiums.

128. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[41]

129. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[42]

130. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[43] 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.[44, 45] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[46]

131. As a result of the Data Breach, Plaintiff and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary

132. To date, Defendants have done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach – Defendants have only

---

[41] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[42] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Sep 13, 2022).

[43] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[44] https://datacoup.com/.

[45] https://digi.me/what-is-digime/.

[46] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

offered 24 months of inadequate identity monitoring services through Experian IdentityWorks, despite Plaintiff and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendants have not offered any other relief or protection.

133. The 24 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. Defendants also place the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

134. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

135. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.[47]

136. Such fraud may go undetected until debt collection calls commence months, or even years, later.

137. Furthermore, the information accessed and disseminated in the Data Breach is

[47] *See* GAO Report, at p. 29.

significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[48] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

138. Consequently, Plaintiff and Class Members are at a imminent and ongoing risk of fraud and identity theft for many years into the future.

139. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

CLASS ACTION ALLEGATIONS

140. 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.

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

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendants Cencora and Lash provided notice to Plaintiff and other Class Members beginning on or around May 17, 2024 (the "Class").

142. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have 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

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

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.

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

144. 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 hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendants' records.

145. 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 Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

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

c. Whether Defendants had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

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

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

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

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. 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.

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

147. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

148. Adequacy of Representation, 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.

149. Superiority, 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 Defendants. 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.

150. 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 Defendants would necessarily gain an unconscionable advantage since it 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 was 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.

151. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, including their privacy policy, uniform methods of data collection, 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.

152. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

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

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

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

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

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

f. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE

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

155. Defendants required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

156. Upon Defendants accepting and storing the Private Information of Plaintiff and Class Members in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected.

157. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

158. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

159. Defendants owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from their failure to so safeguard the Private Information.

160. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their customers/patients, which is recognized by laws and regulations including but not limited to HIPAA and the FTC Act, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

161. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, dental, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

163. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information that they either acquire, maintain, or store.

164. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information, as alleged and discussed above.

165. It was foreseeable that Defendants' failure to use reasonable measures to protect

Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

166. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

167. The imposition of a duty of care on Defendants to safeguard the Private Information they maintained is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

168. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

169. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach in an amount to be determined at trial.

170. Defendants' negligent conduct is ongoing, in that it still holds the Private

Information of Plaintiff and Class Members in an unsafe and unsecure manner.

171. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

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

173. Plaintiff and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable Private Information. Indeed, in acquiring the Private Information, Defendants were then able to charge money for their medical services.

174. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private Information, which cost savings increased the profitability of the services.

175. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their 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 Defendants' failure to provide the requisite security.

176. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that

are mandated by industry standards.

177. Defendants acquired the monetary benefit, Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

178. Had Plaintiff and Class Members known that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants. Plaintiff and Class Members have no adequate remedy at law.

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

180. Furthermore, as a direct and proximate result of Defendants' unreasonable and inadequate data security practices, Plaintiff and Class Members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

181. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

182. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

183. Moreover, Defendants 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, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendants 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 Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information 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, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable

regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing

checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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: May 28, 2024

Respectfully Submitted,

/s/ *Charles E. Schaffer*

Charles E. Schaffer
Nicholas J. Elia
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215)592-1500
Fax: (215)492-4663
cschaffer@lfsblaw.com

nelia@lfsblaw.com

Joseph M. Lyon*
Kevin M. Cox*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
Email: *jlyon@thelyonfirm.com*
Email: *kcox@thelyonfirm.com*

Zachary C. Schaengold*
Cory D. Britt*
Robbins, Kelly, Patterson & Tucker, LPA
312 Elm Street, Suite 2200
Cincinnati, Ohio 45202
T: (513) 721-3330 | F: (513) 721-5001
zschaengold@rkpt.com
cbritt@rkpt.com

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and Putative Class

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

DARLEEN LEWIS

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Charles E. Schaffer, Levin Sedran & Berman LLP, 510 Walnut Street, Suite 500, Philadelphia, PA 19106, (215)592-1500

DEFENDANTS

CENCORA, INC., and THE LASH GROUP, LLC.

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

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

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Negligence arising out of data breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon. Cynthia M. Rufe DOCKET NUMBER 2:24-cv-02227-CMR

DATE 5/28/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Charles E. Schaffer

FOR OFFICE USE ONLY

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

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM
(to be used by counsel to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: Butler County, Ohio

Address of Defendant: 1 West First Avenue, Conshohocken, PA 19428

Place of Accident, Incident or Transaction: Pennsylvania

RELATED CASE IF ANY:
Case Number: 2:24-cv-02227-CMR Judge: Hon. Cynthia M. Rufe Date Terminated N/A

Civil cases are deemed related when ***Yes*** is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes ☒ No ☐
3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes ☐ No ☒

I certify that, to my knowledge, the within case ☒ **is** / ☐ **is not** related to any now pending or within one year previously terminated action in this court except as note above.

DATE: 5/28/2024 /s/ Charles E. Schaffer 76259

Attorney-at-Law (Must sign above) *Attorney I.D. # (if applicable)*

Civil (Place a √ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts)
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Wage and Hour Class Action/Collective Action
- ☐ 6. Patent
- ☐ 7. Copyright/Trademark
- ☐ 8. Employment
- ☐ 9. Labor-Management Relations
- ☐ 10. Civil Rights
- ☐ 11. Habeas Corpus
- ☐ 12. Securities Cases
- ☐ 13. Social Security Review Cases
- ☐ 14. Qui Tam Cases
- ☐ 15. All Other Federal Question Cases. *(Please specify)*:

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☒ 6. Other Personal Injury (*Please specify*): Negligence
- ☐ 7. Products Liability
- ☐ 8. All Other Diversity Cases: *(Please specify)*

ARBITRATION CERTIFICATION
(The effect of this certification is to remove the case from eligibility for arbitration)

I, Charles E. Schaffer, counsel of record *or* pro se plaintiff, do hereby certify:

☒ Pursuant to Local Civil Rule 53.2 § 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

DATE: 5/28/2024 /s/ Charles E. Schaffer 76259

Attorney-at-Law (Sign here if applicable) *Attorney ID # (if applicable)*

NOTE: A trial de novo will be a jury only if there has been compliance with F.R.C.P. 38.