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

AMISH PARIKH, individually and on behalf of all others similarly situated, Plaintiff, v. THE KENDAL CORPORATION, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Amish Parikh ("Plaintiff") brings this Class Action Complaint against The Kendal Corporation ("TKC" or "Defendant"), on behalf of himself individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including, but not limited to, Plaintiff's and Class Members' names, Social Security Numbers, and/or other personal information (collectively, "PII" or "Private Information").

2. TKC is a Delaware-based nonprofit corporation that provides support services to senior living communities.

3. Defendant was subject to a cyberattack between June 26 and June 30, 2024 (the "Data Breach"). Defendant investigated the Data Breach and determined that an unauthorized party gained access to the Private Information of certain TKC employees, including Plaintiff.

4. On or around December 27, 2024, Defendant mailed Plaintiff a letter advising him that the data exposed in the Data Breach included Plaintiff's "name in combination with the following: Social Security number and checking account/routing number provided for direct deposit." Notice of Data Breach, Exhibit A.

5. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information was likely accessed by an unknown third party and precisely what type of information was accessed.

6. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network 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' Personal Information was a known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Personal Information from those risks left that information in a dangerous condition.

7. Because of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

8. By obtaining, collecting, using, and profiting from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted Private Information was impacted during the Data Breach.

9. The exposed Private Information of Plaintiff and Class Members can—and likely will—be sold on the dark web.

10. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

11. This Private Information was compromised because of Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members.

12. For months after Defendant became aware of the Data Breach, Plaintiff and Class Members had no idea their Private Information 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 lifetimes.

13. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injuries because of Defendant's conduct. These injuries include:

(i) lost or diminished value of Private Information;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time; and

(iv) the continued and exacerbated risk to their Private Information which:

a. remains unencrypted and available for unauthorized third parties to access and abuse; and

b. may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded. Defendant further disregarded their rights by failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures for the encryption of data, even for internal use.

16. Because of the Data Breach, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

17. Plaintiff Amish Parikh is a citizen of Lexington, Virginia. He received notice from Defendant that it lost control of his PII.

18. Defendant The Kendal Corporation is a nonprofit corporation formed under the laws of Pennsylvania and having its corporate office at 591 Collaboration Way, Suite 603, Newark, Delaware 19713, with a primary place of business at 1107 E Baltimore Pike Kennett Square, PA 19348.

19. Defendant's registered agent is Corporation Service Company, located Dauphin County, Pennsylvania.

III. JURISDICTION AND VENUE

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

21. This Court has general personal jurisdiction over because Defendant is a corporation formed under the laws of Pennsylvania.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Defendant maintains a location at 1107 E Baltimore Pike Kennett Square, PA 19348.

IV. FACTUAL ALLEGATIONS

The Data Breach

23. In the ordinary course of working for TKC, each employee must provide (and Plaintiff did provide) Defendant with sensitive, personal and private information, including his or her Social Security number, date of birth, and contact information.

24. Defendant agreed to and undertook legal duties to maintain the Private Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

25. Defendant had obligations created by contract, industry standards, common law, and representations made to its clients and to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

26. Defendant agreed to and undertook legal duties to maintain the protected Private Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

27. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

28. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches preceding the date of the breach.

30. As reported by the Identity Theft Resource Center, in 2023 a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[1]

31. 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.

32. In the Notice of Data Breach Defendant mailed to Plaintiff (Exhibit A), Defendant describes the data breach as follows:

> **What Happened?** On June 30, 2024, TKC observed unusual activity on its computer network and immediately began an investigation with the assistance of third-party specialists. The investigation determined that certain files on the TKC network were potentially accessed without authorization between June 26, 2024, and June 30, 2024. The files at issue included information related to current and former employees of TKC and its affiliate care communities. Therefore, TKC reviewed the files at issue to determine the specific information the files contained.
>
> **What Information Was Involved?** TKC has completed its review and determined that the potentially impacted information for current and former employees of TKC and its affiliates included you name in combination [with]

[1] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (*last accessed* November 5, 2024).

the following: Social Security number and checking account/routing number provided for direct deposit.

33. As a consequence of the unauthorized access to Defendant's computer network, Plaintiff's and Class Members' Private Information was exposed to cybercriminals.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

35. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for its intended purposes only, and to make only authorized disclosure of this Private Information.

36. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information, which includes Social Security numbers, information that is static, does not change, and can be used to commit myriad financial crimes.

37. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

39. Because of Defendant's failure to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, an unauthorized third party infiltrated Defendant's systems and stole Plaintiff's and Class Members' Private Information.

40. The unencrypted PII of Plaintiff and Class Members has already been disclosed on the dark web. In addition, unencrypted PII may fall into the hands of companies that will use the

detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

Plaintiff's Experience

41. Plaintiff received a notice from Defendant on or around December 27, 2024, that his Private Information, including his "Social Security number and check account/routing number" was accessed in the Data Breach.

42. Plaintiff is a former employee of TKC.

43. Plaintiff provided Defendant with certain Private Information as a necessary part of his employment.

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

45. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents.

46. Because of the Data Breach, Defendant advised Plaintiff to take certain steps to protect his Private Information and otherwise mitigate his damages.

47. Because of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. And this time was spent at Defendant's direction by way of the Data Breach notice where Defendant recommended that Plaintiff mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

48. In the months since the Data Breach, Plaintiff has experienced an increase in spam phone calls and emails that he attributes to the exposure of his Private Information.

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

50. Plaintiff 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 Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

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

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

Defendant Failed to Comply with FTC Guidelines

53. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

54. 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 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.[2] The guidelines also recommend that businesses use an intrusion detection system to

[2] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 19, 2024).

expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting 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.[3]

55. The FTC further recommends that companies not maintain PII 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.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect client 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 also clarify the measures businesses must take to meet their data security obligations.

57. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to account holders' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Defendant was always fully aware of its obligation to protect the PII of its clients and account holders. Defendant was also aware of the significant repercussions that would result from its failure to do so.

August 19, 2024).
[3] *Id.*

Defendant Failed to Comply with Industry Standards

59. As shown above, experts studying cyber security routinely identify large employers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

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

61. Other best cybersecurity practices that are standard for large, sophisticated employers 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; training staff regarding critical points.

62. Defendant 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.

63. These foregoing frameworks are existing and applicable industry standards for any large employer, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Breach of Duty

64. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect employees' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train employees in the proper email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section *5* of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

65. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing malignant computer code, and inadequately trained employees who opened files containing malware or otherwise left sensitive data exposed, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

66. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

The Risks to Plaintiff and Class Members Created by Defendant's Failure to Safeguard Private Information

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

68. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.

69. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

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

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

considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

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

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

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

75. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

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

numbers are only rising.

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

78. 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.

79. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. 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.

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

81. 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 valuable. Data is currency."[4]

82. The FTC has also issued Many guidelines for businesses that highlight the

[4] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf_(last visited October 6, 2022).

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.

83. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[5] 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.

84. 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 PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

[5] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited October 10, 2022).

85. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

86. The 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. What's more, Defendant places the burden on Plaintiff and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

87. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

88. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

89. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

90. Plaintiff was damaged in that his Private Information is in the hands of cyber criminals.

91. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

92. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

93. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

94. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

95. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

96. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

97. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

98. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

99. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

100. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

V. CLASS ACTION ALLEGATIONS

101. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

102. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the June, 2024 Data Breach (the "Class").**

103. Excluded from the Class are Defendant's officers and directors, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

104. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

105. Numerosity. The Members of the Class are so numerous that joinder of all of them in a single proceeding is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant notified the Maine Attorney General's office that the Data Breach affected 9,810 individuals.

106. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant failed to provide notice of the Data Breach promptly; and

j. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

107. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

108. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

109. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all 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 Defendant's 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.

110. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

111. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this

action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

112. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

113. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

114. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

115. Defendant requires its employees, including Plaintiff and Class Members, to submit non-public personal information in the ordinary course of conducting business.

116. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

117. Defendant 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 its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

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

120. Defendant further had a duty to use reasonable care in protecting confidential data because Defendant is bound by industry standards to protect confidential Private Information.

121. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect timely that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

122. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

123. 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.

124. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

125. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

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

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

127. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

128. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for employment, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

129. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

130. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and adhered to industry standards.

131. Plaintiff and Class Members entrusted their Private Information to Defendant with the reasonable belief and expectation that Defendant would provide adequate data security. Defendant failed to do so.

132. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

133. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

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

135. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

136. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

137. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

138. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its 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.

THIRD COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

139. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

140. Plaintiff brings this claim individually and on behalf of all Class Members. This count is pled in the alternative to the breach of contract count above.

141. Upon information and belief, Defendant funds its data security measures entirely from its general revenue.

142. As such, a portion of the revenue attributable to Plaintiff's and Class Members' labor is to be used to provide a reasonable level of data security.

143. Plaintiff and Class Members conferred a monetary benefit on Defendant. They staffed Defendant's business and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the wages that were the subject of the transaction and appropriate protection for their Private Information.

144. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

145. Defendant enriched itself by saving the costs Defendant reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Rather than providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff

and Class Members by using cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

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

147. Defendant failed to secure Plaintiff's and Class Members' Private Information and thus did not provide full compensation for the benefit Plaintiff and Class Members provided.

148. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices alleged.

149. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

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

151. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the loss of the opportunity to control how their Private Information is used;

c. the compromise, publication, and/or theft of their Private Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

e. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

f. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and

g. future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and Class Members.

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

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

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and his counsel to represent the Class, and finding that Plaintiff is a proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For an Order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Any other relief that this court may deem just and proper.

VIII. JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Date: January 9, 2025

Respectfully submitted,

/s/ Jacob U. Ginsburg
Jacob U. Ginsburg, Esq.
PA Bar ID 311908
Kimmel & Silverman, P.C.
30 East Butler Ave.
Ambler, PA 19002
(267) 468-5374
jginsburg@creditlaw.com
teamkimmel@creditlaw.com

Jarrett L. Ellzey (*pro hac vice* anticipated)
jarrett@ellzeylaw.com
Leigh S. Montgomery (*pro hac vice* anticipated)
lmontgomery@eksm.com
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF AND THOSE SIMILARLY SITUATED

EXHIBIT A

The Kendal Corporation
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PL5DN900201476
AMISH V. PARIKH
[redacted]

KENDAL®
Together, transforming the experience of aging®

December 27, 2024

Notice of Data Breach

Dear Amish Parikh:

The Kendal Corporation ("TKC") writes to notify you of an incident that may affect the privacy of certain information related to current and former employees of TKC and its affiliates. We take this incident seriously and are providing you information about the incident, our response, and steps you can take to help protect your information. The Kendal Corporation has no reason to believe any information has been misused because of this incident.

What Happened? On June 30, 2024, TKC observed unusual activity on its computer network and immediately began an investigation with the assistance of third-party specialists. The investigation determined that certain files on the TKC network were potentially accessed without authorization between June 26, 2024, and June 30, 2024. The files at issue included information related to current and former employees of TKC and its affiliate care communities. Therefore, TKC reviewed the files at issue to determine the specific information the files contained.

What Information Was Involved? TKC has completed its review and determined the potentially impacted information for current and former employees of TKC and its affiliates included your name in combination the following: Social Security number and checking account/routing number provided for direct deposit.

What We Are Doing. In response to this incident, TKC notified law enforcement and conducted a thorough forensic investigation with the assistance of third-party specialists. TKC also reviewed its policies and procedures related to data protection and introduced new technical safeguards to minimize the chance of a similar incident occurring in the future. While TKC has no reason to believe any information has been or will be misused because of this incident, TKC is offering you access to twelve (12) months of complimentary credit monitoring and identity protection services in an abundance of caution.

What You Can Do. If you have not already, we encourage you to enroll in the complimentary credit monitoring and identity protection services we are making available to you. Information about how to enroll in these services along with additional resources available to you are included in the attached *Steps You Can Take to Help Protect Your Information.*

For More Information. We understand you may have questions about this incident. You may contact TKC's dedicated assistance line at **833-799-4337** between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, or write to us at 591 Collaboration Way, Suite 603, Newark, DE 19713.

We regret any concern this incident may cause you.

Sincerely,

The Kendal Corporation

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

Amish Parikh individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Rockbridge Cty, VA
(EXCEPT IN U.S. PLAINTIFF CASES)

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

Kimmel & Silverman, 30 East Butler Pike, Ambler, PA 19002, (215) 540-8888

DEFENDANTS

The Kendal Corporation

County of Residence of First Listed Defendant Chester 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

TORTS

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

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

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

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

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

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

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

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

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

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

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

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

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

PRISONER PETITIONS

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Defendant suffered a data breach, which damaged a class of individuals whose personal information was stolen.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 1/8/2025

SIGNATURE OF ATTORNEY OF RECORD /s/ Jacob Ginsburg

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket. **PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related cases, if any. If a related case exists, whether pending or closed, insert the docket numbers and the corresponding judge names for such cases. A case is related to this filing if the case: 1) involves some or all of the same parties and is based on the same or similar claim; 2) involves the same property, transaction, or event; 3) involves substantially similar issues of law and fact; and/or 4) involves the same estate in a bankruptcy appeal.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM

Place of Accident, Incident, or Transaction: Pennsylvania, Virginia

RELATED CASE IF ANY: Case Number:_____ Judge:_____

1. Does this case involve property included in an earlier numbered suit? Yes ☐
2. Does this case involve a transaction or occurrence which was the subject of an earlier numbered suit? Yes ☐
3. Does this case involve the validity or infringement of a patent which was the subject of an earlier numbered suit? Yes ☐
4. Is this case a second or successive habeas corpus petition, social security appeal, or pro se case filed by the same individual? Yes ☐
5. Is this case related to an earlier numbered suit even though none of the above categories apply? If yes, attach an explanation. Yes ☐

I certify that, to the best of my knowledge and belief, the within case ☐ **is** / ☒ **is not** related to any pending or previously terminated action in this court.

Civil Litigation Categories

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. Cases Seeking Systemic Relief ***see certification below***
- ☐ 16. 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*): Data breach
- ☐ 7. Products Liability
- ☐ 8. All Other Diversity Cases: *(Please specify)*_____

I certify that, to the best of my knowledge and belief, that the remedy sought in this case ☒ **does** / ☐ **does not** have implications beyond the parties before the court and ☐ **does** / ☒ **does not** seek to bar or mandate statewide or nationwide enforcement of a state or federal law including a rule, regulation, policy, or order of the executive branch or a state or federal agency, whether by declaratory judgment and/or any form of injunctive relief.

ARBITRATION CERTIFICATION (CHECK ONLY ONE BOX BELOW)

I certify that, to the best of my knowledge and belief:

☒ Pursuant to Local Civil Rule 53.2(3), this case is not eligible for arbitration either because (1) it seeks relief other than money damages; (2) the money damages sought are in excess of $150,000 exclusive of interest and costs; (3) it is a social security case, includes a prisoner as a party, or alleges a violation of a right secured by the U.S. Constitution, or (4) jurisdiction is based in whole or in part on 28 U.S.C. § 1343.

☐ None of the restrictions in Local Civil Rule 53.2 apply and this case is eligible for arbitration.

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