

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TENNESSEE  
SOUTHERN DIVISION**

**MICHAEL HARRIS, *individually and  
on behalf of others similarly situated,***

**Plaintiff,**

v.

**LEE UNIVERSITY,**

**Defendant.**

**CASE NO.**

**CLASS ACTION COMPLAINT**

Plaintiff Michael Harris (“Plaintiff”), by and through undersigned counsel, on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the “Action”) against Defendant Lee University (“LU” or “Defendant”) upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

**I. SUMMARY**

1. Plaintiff brings this Action on behalf of himself and all other similarly situated victims as a result of a recent cyberattack and data breach involving the personally identifiable information suffered by Lee University.

2. In or around March 2024, an unknown and unauthorized criminal actor gained access to Defendant’s network and exfiltrated, at a minimum, names, Social Security numbers, and/or education-related information. (“PII”)<sup>1</sup>.

---

<sup>1</sup> Notice of Data Security Incident, attached hereto as **Exhibit A**.

3. In the Notice of Data Security Incident letter Defendant sent to Plaintiff and Class Members on or around March 24, 2025, Defendant explains<sup>2</sup>:

**What Happened.** In March 2024, we experienced a security incident that impacted our local systems through a third-party software vulnerability. After detecting the third-party vulnerability and containing the incident, we launched an investigation with the support of industry-leading cybersecurity experts to learn more about the scope of the potentially affected data on those systems. Our investigation revealed that some university data may have been downloaded from our systems. We then launched a comprehensive review of all potentially affected data to try to identify individuals whose information was involved and gather contact information needed to provide notice. These efforts concluded in March 2025. After we learned that some of your information was potentially involved, we arranged to provide you this notice.

**What Information Was Involved.** The potentially involved information varies by individual. Based on the investigation, we understand that the information may have included your name, Social Security number, and/or education-related information.

**What We Are Doing.** As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

4. To be clear – there are numerous issues with LU’s Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1.) LU waited over *one year* to notice Plaintiff and Class members of the Data Breach; (2.) LU fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the PII that LU continues to maintain is secure; and (3.) LU fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

---

<sup>2</sup> *Id.*

5. Furthermore, Defendant's delay in notifying Plaintiff and Class members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification statute in Tennessee. *See* TN Code § 47-18-2107 which requires that the disclosure notification be made "no later than forty-five (45) days from the discovery or notification of the breach." Defendant failed to meet this requirement by over **300 days**.

6. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

7. In addition, Plaintiff's and Class Members' sensitive PII—which was entrusted to Defendant — was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains also in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to future cyberattacks and theft.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

10. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

11. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

12. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff and Class members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

13. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for months or even years.

14. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

15. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

19. Plaintiff seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

20. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of himself and the putative Class.

## **II. JURISDICTION AND VENUE**

21. 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 exact number of class members is unknown to Plaintiff, but upon information and belief exceeds 100, and at least one Class member is a citizen of a state that is

diverse from Defendant's citizenship, namely Plaintiff a citizen of North Carolina. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has personal jurisdiction over Defendant Lee University because its principal place of business is in Tennessee, and it does a significant amount of business in Tennessee.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant Lee University has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

### **III. PARTIES**

#### ***Plaintiff Michael Harris***

24. Plaintiff Michael Harris is an individual citizen of North Carolina and received a letter from Defendant notifying him of the Data Breach on or around March 24, 2025. Plaintiff Harris's data was exposed because he was a prospective student of Lee University.

#### ***Defendant Lee University***

25. Defendant Lee University is a Tennessee corporation with its principal place of business located in Cleveland, Tennessee. Defendant is an undergraduate and graduate Christian university.

### **IV. FACTUAL ALLEGATIONS**

#### ***Defendant's Business***

26. According to Defendant Lee University's website:

Lee is a Christian institution which offers liberal arts and professional education on both the undergraduate and graduate levels through residential and distance programs.<sup>3</sup>

---

<sup>3</sup> <https://www.leeuniversity.edu/about/mission/> (last accessed April 1, 2025)

27. Defendant collects personally identifiable information in the course of doing business. This personally identifiable information includes the PII which was compromised in the Data Breach alleged herein.

28. Prior to requesting and receiving information from Lee University, Plaintiff and Class Members were required to and did in fact turn over their PII to LU.

29. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

30. As a condition of receiving information from LU, LU requires that Plaintiff and Class Members entrust it with highly sensitive personal information.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

32. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

33. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

### ***The Attack and Data Breach***

34. On March 24, 2025, Defendant informed Plaintiff and the Class Members of the Data Breach via a letter explaining the following:

**What Happened.** In March 2024, we experienced a security incident that impacted our local systems through a third-party software vulnerability. After detecting the third-party vulnerability and containing the incident, we launched an investigation with the support of industry-leading cybersecurity experts to learn more about the scope of the potentially affected data on those systems. Our investigation revealed that some university data may have been downloaded from our systems. We then launched a comprehensive review of all potentially affected data to try to identify individuals whose information was involved and gather contact information needed to provide notice. These efforts concluded in March 2025. After we learned that some of your information was potentially involved, we arranged to provide you this notice.

**What Information Was Involved.** The potentially involved information varies by individual. Based on the investigation, we understand that the information may have included your name, Social Security number, and/or education-related information.

**What We Are Doing.** As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.<sup>4</sup>

35. The personally identifiable information that was compromised includes, but is not limited to full name, Social Security number, and/or education-related information.

36. The Notice letter also states that LU is offering victims of the Data Breach credit monitoring services.<sup>5</sup> With its offer of credit monitoring services, Defendant is acknowledging that Plaintiff and Class Members are subject to an imminent threat of identity theft and financial fraud.

---

<sup>4</sup> Exhibit A.

<sup>5</sup> *Id.*



37. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

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

39. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal and financial data from its many current, former, and prospective students, including Plaintiff and Class Members.

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

41. Defendant had obligations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

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

43. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information, including through its privacy policies.<sup>6</sup>

***The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk***

44. It is well known that PII, including Social Security numbers and names in particular are invaluable commodities and a frequent target of hackers.

---

<sup>6</sup> See <https://www.leeuniversity.edu/privacy-policy/> ("We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process.") (last accessed April 1, 2025).

45. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.<sup>7</sup>

46. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes “significant negative financial impact on victims” as well as severe distress and other strong emotions and physical reactions.

47. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the “secret sauce” that is “as good as your DNA to hackers.” There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that “a new number probably won’t solve all [] problems ... and won’t guarantee ... a fresh start.”<sup>8</sup>

48. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), and, in light of the recent data breaches Wells Fargo has suffered, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

<sup>7</sup> ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), available at <https://www.idtheftcenter.org/publication/2023-data-breach-report/> (last accessed April 1, 2025).

<sup>8</sup> See Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed April 1, 2025).

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

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

***Defendant Had A Duty to Plaintiff and Class Members to Secure Private Information***

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

52. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class relied on Defendant to secure their PII when they entrusted Defendant with the information required to request and receive information from LU.

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

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

- a. Maintaining a secure firewall configuration;
- b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- c. Monitoring for suspicious or irregular traffic to servers;
- d. Monitoring for suspicious credentials used to access servers;
- e. Monitoring for suspicious or irregular activity by known users;
- f. Monitoring for suspicious or unknown users;
- g. Monitoring for suspicious or irregular server requests;
- h. Monitoring for server requests for PII;
- i. Monitoring for server requests from VPNs; and
- j. Monitoring for server requests from Tor exit nodes.

55. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>9</sup> 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.”<sup>10</sup>

56. The ramifications of Defendant’s failure to keep PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims is likely to continue for years.

---

<sup>9</sup> 17 C.F.R. § 248.201 (2013).

<sup>10</sup> *Id.*

### *The Value of Personally Identifiable Information*

57. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>11</sup> 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.<sup>12</sup>

58. As a growing number of federal courts have begun to recognize the loss of value of PII as a viable damages theory, the sale of PII from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

59. The dark net is an unindexed layer of the internet that requires special software or authentication to access.<sup>13</sup> 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

---

<sup>11</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed April 1, 2025).

<sup>12</sup> *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: <https://www.privacyaffairs.com/dark-web-price-index-2021/> (last accessed April 1, 2025).

<sup>13</sup> *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last accessed April 1, 2025).

ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.<sup>14</sup> This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

60. 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 PII at issue here.<sup>15</sup> The digital character of PII 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.<sup>16</sup> As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”<sup>17</sup>

61. Plaintiff and Class Members’ PII is a valuable commodity, a market exists for Plaintiff and Class Members’ PII (which is why the Data Breach was perpetrated in the first place), and Plaintiff and Class Members’ PII is being likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiff and Class Members have lost the value of their PII, which is sufficient to plausibly allege injury arising from a data breach.

62. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>18</sup> In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker

---

<sup>14</sup> *Id.*

<sup>15</sup> *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web> (last accessed April 1, 2025).

<sup>16</sup> *Id.*; *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>(last accessed April 1, 2025).

<sup>17</sup> *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web> (last accessed April 1, 2025).

<sup>18</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed April 1, 2025).

who in turn aggregates the information and provides it to marketers or app developers.<sup>1920</sup> Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>21</sup>

63. The PII stolen in this specific Data Breach was particularly harmful. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

64. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

65. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>22</sup>

66. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

<sup>19</sup> <https://datacoup.com/> (last accessed April 1, 2025).

<sup>20</sup> <https://digi.me/about-us> (last accessed April 1, 2025).

<sup>21</sup> Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqn.html> (last accessed April 1, 2025).

<sup>22</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed April 1, 2025).

67. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>23</sup>

68. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>24</sup>

69. PII can be used to distinguish, identify, or trace an individual’s identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.<sup>25</sup>

70. Given the nature of Defendant’s Data Breach, as well as the unreasonable delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff’s and Class Members’ PII can easily obtain Plaintiff’s and Class Members’ tax returns or open fraudulent credit card accounts in Class Members’ names.

71. 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

---

<sup>23</sup> Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed April 1, 2025).

<sup>24</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed April 1, 2025).

<sup>25</sup> See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.



breach, because credit card victims can cancel or close credit and debit card accounts.<sup>26</sup> The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers and dates of birth).

72. To date, Defendant has offered its victims *only one year* of identity monitoring services. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

73. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures.

### *Plaintiff’s Experience*

74. Plaintiff was required to provide and did provide his PII to Defendant as a condition of requesting and receiving information from LU.

75. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff’s PII has already been “impacted” in the Data Breach and likely been made available on the dark web to anyone wishing to purchase it.

76. The fraud and identity monitoring services offered by Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service.

77. Nor has Defendant compensated Plaintiff and Class Members for the time they will spend monitoring their accounts, placing credit freezes and fraud alerts, changing online passwords and other actions.

---

<sup>26</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, available at: [https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1\\_\(last accessed April 1, 2025\)](https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1_(last%20accessed%20April%201,%202025)).

78. Plaintiff and Class Members have been further damaged by the compromise of their PII in the Data Breach which was “impacted” and is in the hands of cybercriminals who illegally accessed Defendant’s network for the specific purpose of targeting the PII.

79. Plaintiff typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

80. Plaintiff stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

81. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent significant time monitoring his accounts and credit score, changing his online account passwords and verifying the legitimacy of the Notice and researching the Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

82. Specifically, since the date of the breach Plaintiff has spent over twenty-four (24) hours taking action to mitigate the harm he has suffered. Plaintiff (1) has spent, and continues to spend, considerable time and effort actively monitoring his accounts and credit; and (2) he has lost sleep due to the stress and anxiety he now suffers from the fear of his PII being exposed, misused and sold on the black market.

83. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII — a form of intangible property that he entrusted to Defendant for the purpose of receiving information from LU, which was compromised in and as a result of the Data Breach.

84. 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 his privacy.

85. Plaintiff suffered emotional distress and increased stress and anxiety as a result of the Data Breach because of the actions he has been forced to undertake, the loss of control over his most intimate information, and the fact that he must remain vigilant for the remainder of his life.

86. Plaintiff has suffered imminent and impending injury arising from the increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

87. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff as a condition of requesting and receiving information from LU. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

88. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

## **V. CLASS ACTION ALLEGATIONS**

89. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil, which is preliminarily defined as:

All persons Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the “Class”).

90. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

91. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, thousands of individuals have been affected by this breach. The identities of Class Members are ascertainable through Defendant’s records, Class Members’ records, publication notice, self-identification, and other means.

92. **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:

- i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff’s and Class Members’ PII;
- ii. 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;
- iii. Whether Defendant’s data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- iv. Whether Defendant’s data security systems prior to and during the Data Breach were consistent with industry standards;

- v. Whether Defendant owed a duty to Class Members to safeguard their PII;
- vi. Whether Defendant breached its duty to Class Members to safeguard their PII;
- vii. Whether computer hackers obtained Class Members' PII in the Data Breach;
- viii. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- ix. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- x. Whether Defendant's conduct was negligent; and;
- xi. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

93. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

94. **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.

95. **Predominance.** Defendant has 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 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.

96. **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. 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.

97. 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.

98. Likewise, particular issues under Federal 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:

- xii. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- xiii. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- xiv. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

xv. Whether Defendant failed to take commercially reasonable steps to safeguard PII,

99. 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**

### **COUNT I NEGLIGENCE (On Behalf of Plaintiff and the Class)**

100. Plaintiff hereby repeats and realleges paragraphs 1 through 99 of this Complaint and incorporates them by reference herein.

101. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

102. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

103. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. The harm that Plaintiff and Class Members experienced was within the zone of foreseeable harm known to Defendant.

104. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiff and the Class. That special

relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in requesting and receiving information from LU. While this special relationship exists independent from any contract, it is recognized by Defendant's privacy practices, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered PII as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

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

107. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was foreseeable that Plaintiff and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

108. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included



its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

109. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

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

111. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII 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 they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

113. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

115. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

116. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), Defendant had a separate and independent duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

117. The FTCA is intended, in part, to protect individuals whose PII is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

118. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect as their PII was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

119. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

120. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the members of the Class.

121. Defendant breached its duties to Plaintiff and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

122. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

123. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the members of the Class, they would not have been injured.

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

126. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be

expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

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

128. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

129. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

130. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief to be determined at trial.

**COUNT II**  
**BREACH OF IMPLIED CONTRACT**  
**(On Behalf of Plaintiff and the Class)**

131. Plaintiff hereby repeats and realleges paragraphs 1 through 99 of this Complaint and incorporates them by reference herein.

132. Plaintiff and the Class entrusted their PII to Defendant as a condition of requesting and receiving information from LU. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information,

to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

133. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

134. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

135. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

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

137. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and

economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

139. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

**COUNT III**  
**INVASION OF PRIVACY – INTRUSION UPON SECLUSION**  
**(On Behalf of Plaintiff and the Class)**

140. Plaintiff hereby repeats and realleges paragraphs 1 through 99 of this Complaint and incorporates them by reference herein.

141. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

142. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

143. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise

to the Data Breach were intentional in that the decisions to implement lax security and failure to timely notice Plaintiff and the Class were undertaken willfully and intentionally.

144. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

- a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;
- b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;
- c. failing to adequately secure their PII from disclosure to unauthorized persons; and
- d. enabling the disclosure of their PII without consent.

145. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded and private data.

146. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

147. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

148. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

149. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

150. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

**COUNT IV**  
**UNJUST ENRICHMENT/QUASI CONTRACT**  
**(On Behalf of Plaintiff and the Class)**

151. Plaintiff hereby repeats and realleges paragraphs 1 through 99 of this Complaint and incorporates them by reference herein.

152. This Count is brought in the alternative to Count II, Breach of Implied Contract.

153. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

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

155. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant 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 Defendant's failure to provide the requisite security.

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

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

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

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

160. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to

prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

161. 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.

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

## **VII. PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

- a.) For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;
- b.) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Breach;
- d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

- f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;
- g.) For an award of punitive damages, as allowable by law;
- h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i.) Pre- and post-judgment interest on any amounts awarded and,
- j.) All such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMAND**

Plaintiff hereby demands a trial by jury.

DATED: April 1, 2025

Respectfully submitted,

**SHAMIS & GENTILE P.A.**

/s/ Andrew Shamis  
Andrew J. Shamis, Esq.  
[ashamis@shamisgentile.com](mailto:ashamis@shamisgentile.com)  
14 NE 1st Ave., Suite 705  
Miami, Florida 33132  
Tel: (305) 479-2299

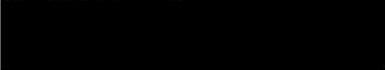
# EXHIBIT A



Return to IDX  
P.O. Box 989728  
West Sacramento, CA 95798-9728



Michael Harris



March 24, 2025

**Subject: Notice of Data Security Incident**

Dear Michael Harris,

We are writing to inform you of a recent data security incident that may have involved your information. Lee University takes the privacy and security of all information in our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

**What Happened.** In March 2024, we experienced a security incident that impacted our local systems through a third-party software vulnerability. After detecting the third-party vulnerability and containing the incident, we launched an investigation with the support of industry-leading cybersecurity experts to learn more about the scope of the potentially affected data on those systems. Our investigation revealed that some university data may have been downloaded from our systems. We then launched a comprehensive review of all potentially affected data to try to identify individuals whose information was involved and gather contact information needed to provide notice. These efforts concluded in March 2025. After we learned that some of your information was potentially involved, we arranged to provide you this notice.

**What Information Was Involved.** The potentially involved information varies by individual. Based on the investigation, we understand that the information may have included your name, Social Security number, and/or education-related information.

**What We Are Doing.** As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

**What You Can Do.** You can follow the recommendations on the following page to help protect your information. We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-877-719-6522, visiting <https://app.idx.us/account-creation/protect> or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 24, 2025.

UNITED STATES DISTRICT COURT

for the

Eastern District of Tennessee

MICHAEL HARRIS, individually and on behalf of others similarly situated

Plaintiff(s)

v.

LEE UNIVERSITY

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) LEE UNIVERSITY R/A CHRIS H CONINE 1120 N OCOEE ST CLEVELAND, TN 37311

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Shamis & Gentile, P.A. 14 NE 1st Avenue, Suite 705 Miami, FL 33132

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: \_\_\_\_\_

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*:

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00 .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

# 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.)

<b>I. (a) PLAINTIFFS</b> MICHAEL HARRIS, individually and on behalf of others similarly situated  <b>(b)</b> County of Residence of First Listed Plaintiff <u>Fayetteville, NC</u> <i>(EXCEPT IN U.S. PLAINTIFF CASES)</i>  <b>(c)</b> Attorneys <i>(Firm Name, Address, and Telephone Number)</i> SHAMIS & GENTILE P.A., 14 NE 1st Ave., Suite 705, Miami, Florida 33132, Tel: (305) 479-2299	<b>DEFENDANTS</b>  LEE UNIVERSITY  County of Residence of First Listed Defendant <u>Cleveland, TN</u> <i>(IN U.S. PLAINTIFF CASES ONLY)</i> NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.  Attorneys <i>(If Known)</i>
---	--

<b>II. BASIS OF JURISDICTION</b> <i>(Place an "X" in One Box Only)</i>  <input type="checkbox"/> 1 U.S. Government Plaintiff <input type="checkbox"/> 2 U.S. Government Defendant <input type="checkbox"/> 3 Federal Question <i>(U.S. Government Not a Party)</i> <input checked="" type="checkbox"/> 4 Diversity <i>(Indicate Citizenship of Parties in Item III)</i>	<b>III. CITIZENSHIP OF PRINCIPAL PARTIES</b> <i>(Place an "X" in One Box for Plaintiff and One Box for Defendant)</i>  <table style="width:100%; border-collapse: collapse;"> <tr> <td style="width:25%;"></td> <td style="width:10%; text-align: center;"><b>PTF</b></td> <td style="width:10%; text-align: center;"><b>DEF</b></td> <td style="width:45%;"></td> <td style="width:10%; text-align: center;"><b>PTF</b></td> <td style="width:10%; text-align: center;"><b>DEF</b></td> </tr> <tr> <td>Citizen of This State</td> <td style="text-align: center;"><input type="checkbox"/> 1</td> <td style="text-align: center;"><input type="checkbox"/> 1</td> <td>Incorporated or Principal Place of Business In This State</td> <td style="text-align: center;"><input type="checkbox"/> 4</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 2</td> <td style="text-align: center;"><input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business In Another State</td> <td style="text-align: center;"><input type="checkbox"/> 5</td> <td style="text-align: center;"><input type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td style="text-align: center;"><input type="checkbox"/> 3</td> <td style="text-align: center;"><input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td style="text-align: center;"><input type="checkbox"/> 6</td> <td style="text-align: center;"><input type="checkbox"/> 6</td> </tr> </table>		<b>PTF</b>	<b>DEF</b>		<b>PTF</b>	<b>DEF</b>	Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4	Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	<b>PTF</b>	<b>DEF</b>		<b>PTF</b>	<b>DEF</b>																				
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4																				
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5																				
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																				

<b>IV. NATURE OF SUIT</b> <i>(Place an "X" in One Box Only)</i>					<a href="#">Click here for: Nature of Suit Code Descriptions.</a>
<b>CONTRACT</b>	<b>TORTS</b>	<b>FORFEITURE/PENALTY</b>	<b>BANKRUPTCY</b>	<b>OTHER STATUTES</b>	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input checked="" type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<b>PERSONAL INJURY</b> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<b>PERSONAL INJURY</b> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability  <b>PERSONAL PROPERTY</b> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other  <b>LABOR</b> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act  <b>IMMIGRATION</b> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157  <b>INTELLECTUAL PROPERTY RIGHTS</b> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016  <b>SOCIAL SECURITY</b> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))  <b>FEDERAL TAX SUITS</b> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<b>REAL PROPERTY</b>	<b>CIVIL RIGHTS</b>	<b>PRISONER PETITIONS</b>			
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<b>Habeas Corpus:</b> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty  <b>Other:</b> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

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

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

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:  
 28 U.S.C. § 1332(d)(2).

Brief description of cause:  
 Breach of contract

**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: April 1, 2025      SIGNATURE OF ATTORNEY OF RECORD: /s/ Andrew J Shamis



## 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 pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- Date and Attorney Signature.** Date and sign the civil cover sheet.