UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA
PITTSBURGH DIVISION

ERIN HETTMAN, on behalf of himself and all others similarly situated, Plaintiff, v. **ECKERT SEAMANS CHERIN & MELLOTT, LLC** Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Erin Hettman ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Eckert Seamans Cherin & Mellott, LLC ("Eckert Seamans" or "Defendant"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

INTRODUCTION

1. This class action arises from Eckert Seaman's failure to protect highly sensitive data of at least 9,400 alumni of Wheeling Jesuit University in a cybersecurity incident beginning on or around April 17, 2025, and lasting for an unknown period of time. During the Data Breach, files were "copied," or stolen, from Eckert Seaman's computer network.

2. Eckert Seaman is a law firm that *formerly* represented Wheeling Jesuit University in legal proceedings. Despite the fact that Eckert Seaman had no legitimate reason to maintain the data it collected from Wheeling Jesuit University alumni in the course of its representation, it nevertheless maintained and stored the highly sensitive Private Identifying Information ("PII") of thousands of Wheeling Jesuit University alumni in an unencrypted format.

3. Plaintiff is an alumnus of Wheeling Jesuit University and a Data Breach victim, having received Notice of the Data Breach in June 2025.

4. It is unclear when Eckert Seamans discovered it had lost control over its computer network and realized that cybercriminals accessed highly sensitive personal information stored on its computer network. In the Notice it sent to Data Breach victims, including Plaintiff, Defendant claims it became aware of suspicious activity on April 17, 2025, and "quickly contained this incident." Exhibit A. However, Eckert Seaman reported to the Attorney General of Maine that it did not discover the Data Breach until May 20, 2025.[1]

5. Following an internal investigation, Defendant learned that "an unauthorized actor accessed the attorney's computer and a limited amount of firm data that the attorney had access to on Eckert Seaman's network and then copied some of those files, including a 2019 document identifying Wheeling Jesuit alumni." In other words, a cybercriminal stole files containing the PII of Wheeling Jesuit alumni.

6. While Defendant has not publicly released the categories of the compromised data, it is fair to assume that the compromised data included at least names, Social Security numbers, Driver's license or state identification card numbers, financial account information, and/or account passwords or personal identification numbers or other access codes, given the Maine state reporting guidelines.

7. On or about June 18, 2025—approximately 2 months after the Data Breach—Eckert Seamans finally began notifying Class Members about the Data Breach.

[1] *See Data Breach Notification*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/de6640e0-abfe-4d3f-b360-899e7aa88a61.html (last visited July 25, 2025).

8. Upon information and belief, cybercriminals were able to breach Defendant's systems over an unknown period of time (and for perhaps 33 days) because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering it an easy target for cybercriminals.

9. Defendant's Notice intentionally obfuscates the nature of the Data Breach and the threat it posed. The Notice failed to disclose how many people were impacted, how the Data Breach happened, who perpetrated the breach, whether a ransom was demanded or paid, when it was able to secure its systems, or why it took the Defendant approximately two months before it finally began notifying some victims that cybercriminals had gained access to their highly private information. Additionally, the information contained within Defendant's Notice contradicts the representations Defendant made to the Attorney General of Maine.

10. Defendant further claims in its Notice that "we are not aware of any misuse of your information," but failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

11. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff's and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

12. Moreover, Defendant's deliberate failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

13. In failing to adequately protect its current and former clients' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed at least 9,400 individuals.

14. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant and/or their agent Wheeling Jesuit University with their PII. But Defendant betrayed that trust when Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

15. Plaintiff Erin Hettman is an alumnus of Wheeling Jesuit University and victim of the Data Breach. At least his name and Social Security number were exposed to cybercriminals during the Data Breach.

16. Defendant had no legitimate reason to maintain Ms. Hettman's PII, considering he is no longer a student of Wheeling Jesuit University, and Wheeling Jesuit University is no longer Defendant's client.

17. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

18. Plaintiff Erin Hettman is a natural person and citizen of Core, West Virgina, where he intends to remain.

19. Defendant Eckert Seamans, is a Pennsylvania-based domestic restricted professional limited liability company with its headquarters and principal place of business at 600 Grant St. 44th Fl, Pittsburgh, PA 15219

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. Members of the proposed Class are citizens of different states than Defendant and there are over 100 putative Class members. After all, at least 9,400 persons were affected, including persons residing in at least the following states: West Virginia, Maine, and Vermont.[2]

21. This court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts with this State.

22. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

[2] *See Data Breach Notification*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/de6640e0-abfe-4d3f-b360-899e7aa88a61.html (last visited July 25, 2025) *and Data Breach Notice to Consumers,* VERMONT.GOV, https://ago.vermont.gov/document/2025-06-18-eckert-seamans-cherin-mellott-data-breach-notice-consumers (last visited July 25, 2025).

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

23. Eckert Seamans is a national law practice with offices across the United States. It was founded in 1958 and employs approximately 650 individuals. As a litigation law firm, Eckert Seamans specializes in corporate and business law, intellectual property law, labor and employment relations, hospitality and gaming law, aviation, and more.

24. Headquartered in Pittsburgh, Pennsylvania, Eckert Seamans has locations in Massachusetts, Washington D.C., Delaware, New York, New Jersey, Virginia, Michigan, Connecticut, Rhode Island, and West Virginia.

25. On information and belief, Eckert Seamans accumulates highly private PII of its clients, including Social Security numbers. Given its age, Eckert Seamans has accrued over 65 years of data.

26. In collecting and maintaining its clients' PII, Eckert Seamans agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

27. Eckert Seamans understood the need to protect its current and former clients' PII and prioritize its data security.

28. Eckert Seamans states, "If you a current or former client of ESCM, we do not knowingly disclose Personal Information about you in the course of representing you, except as expressly or impliedly authorized by you to enable us to effectuate the purpose of our representation or as required or permitted by law or applicable provisions of codes of professional responsibility or ethical rules governing our conduct as lawyers. Except as noted herein, ESCM

does not knowingly disclose Personal Information to any person or entity outside of ESCM."[3] It follows that secure and reliable data storage should be deeply important to Eckert Seamans.

29. Despite recognizing its duty to do so, on information and belief, Eckert Seamans has not implemented reasonable cybersecurity safeguards or policies to protect the PII of its current and former clients, or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Eckert Seamans leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to clients' PII.

Defendant Failed to Safeguard the PII of Plaintiff and the Class

30. Plaintiff is an alumnus of Wheeling Jesuit University and Data Breach Victim.

31. As a condition of attending Wheeling Jesuit University, Plaintiff provided his PII to Wheeling Jesuit University. In the course of unidentified legal proceedings, Wheeling Jesuit University provided Plaintiff's PII to Defendant.

32. On information and belief, Defendant collects and maintains its clients' unencrypted PII in its computer systems.

33. In collecting and maintaining PII, Defendant implicitly and explicitly agreed that it will safeguard the data using reasonable means according to state and federal law.

34. From April 17, 2025 to May 20, 2025, cybercriminals hacked Defendant's network and accessed extremely sensitive information, including social security numbers.

35. Based on the conflicting information Defendant reported to the Attorney General of Maine and to consumers, it is unclear how long the Data Breach lasted.

36. Regardless of whether the cybercriminals had access to Defendant's computer network for a day or thirty-three days, the Data Breach demonstrates Defendant's cyber and data

[3] *Privacy Policy,* ECKERT SEAMANS, https://www.eckertseamans.com/our-firm/about-our-firm (last visited June 30, 2025).

security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its clients' highly private information continuously over the course of two months.

37. Nevertheless, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner. In so doing, Defendant has deprived Plaintiff and the Class of the earliest opportunity to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

38. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing clients' PII, as evidenced by the Data Breach. In fact, Defendant did not even delete the PII of its former clients, although it had no legitimate reason the highly private PII of its former client's alumni.

39. Defendant's failure to adopt adequate cybersecurity measures demonstrates that there is a substantial risk of another breach of its systems, or that another breach is certainly impending.

40. Even with the purchase of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff and the Class's financial accounts.

42. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its clients' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach, and to stop cybercriminals from accessing the PII it stored in its network.

43. Furthermore, Defendant intentionally obfuscates the nature of the breach, failing to clearly inform the public how many people were impacted, how the Data Breach happened, who perpetrated the breach, whether a ransom was demanded or paid, when it was able to secure its systems, or why it took the Defendant approximately two months before it finally began notifying some victims that cybercriminals had gained access to their highly private information. Additionally, the information contained within Defendant's Notice contradicts the representations Defendant made to the Attorney General of Maine.

44. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts.

45. Despite Defendant's intentional opacity about the root cause of the data breach and its impact, several facts can be gleaned from the notice including that: (1) this data breach was the work of cybercriminals; (2) cybercriminals successfully infiltrated Eckert Seamans's network environment; and (3) once inside, cybercriminals targeted highly private information for download and theft.

46. Companies only send notice letters because data breach notification laws require them to do so, and notice letters are only sent to those persons who Defendant itself reasonably believes had PII acquired by an unauthorized individual.

47. By sending notice letters to Plaintiff and Class Members, Defendant admits that it

itself reasonably believes Plaintiff's PII, including his Social Security number, was acquired by an unnamed third party.

Defendant Knew—or Should Have Known—of the Risk of a Data Breach

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

49. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

50. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[4]

51. 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. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[5]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the construction industry, including Defendant.

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

---

[4] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited July 25, 2025).

[5] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 25, 2025).

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

55. In light of the information readily available and accessible before the Data Breach, Defendant, knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

Plaintiff's Experience and Injuries

56. Plaintiff is an alumnus of Wheeling Jesuit University and a Data Breach victim, having received Notice of the Data Breach in June 2025. At minimum, Plaintiff's full name and Social Security number were stolen during the Data Breach.

57. As a condition of attending Wheeling Jesuit University, Plaintiff was required to provide his PII, including at least his name, date of birth, address, Social Security Number, and health information. As a condition of receiving legal services from Defendant, Wheeling Jesuit University was required to provide to Defendant the PII of its students.

58. Plaintiff provided his PII to Wheeling Jesuit University and trusted that the University would use reasonable measures to protect it according to state and federal law. Likewise, Wheeling Jesuit University provided Plaintiff's PII to Defendant and trusted that the law firm would maintain client-confidential and use reasonable measures to protect the PII entrusted to its safekeeping.

59. Additionally, Plaintiff reasonably expected that his personal information would not be maintained for an unreasonable amount of time. Plaintiff has not attended Wheeling Jesuit University for over two decades, and does not understand why Defendant still maintained his PII.

60. Had Plaintiff known that Defendant does not adequately protect PII, he would not have agreed to provide his PII to Wheeling Jesuit University or Defendant. Additionally, had Plaintiff known that Defendant would not delete his PII once their business relationship had ended, he would not have agreed to provide his PII to Wheeling Jesuit University or Defendant.

61. Plaintiff received Notice of the Data Breach in June 2025. Plaintiff was surprised to have received this Notice, considering he has not been a student of the University for over two decades, and does not know why the university entrusted Defendant with his PII. Defendant should not have stored Plaintiff's PII beyond the time necessary to achieve its initial purpose of collection. Defendant had no need of Plaintiff's Social Security number at the time of the Data Breach, and should have promptly deleted it.

62. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Wheeling Jesuit University or Defendant had he known of Defendant's lax data security policies.

63. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

64. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Data Breach.

65. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

66. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

67. Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information.

68. Plaintiff will continue to spend valuable time he would have otherwise spent on other activities, including but not limited to, work and/or recreation. Plaintiff's efforts were reasonable and necessary given Defendant instructed Plaintiff to "remain vigilant for incidents of fraud and identity theft." Exhibit A.

69. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Plaintiff is experiencing anxiety, distress, and fear regarding how the exposure and loss of his Social Security number will impact her. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

70. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury is worsened by the fact Defendant had no legitimate reason to maintain his PII.

71. Once an individual's PII is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[6] Plaintiff's name and Social Security number were compromised as a result of the Data Breach.

72. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendant's possession despite the fact he is no longer enrolled at the University and the University is no longer a client of Defendant, is protected and safeguarded from future breaches.

Plaintiff and the Class Suffered Common Injuries and Damages Due to Defendant's Conduct

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

74. As a result of Defendant's failure to prevent 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. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. Identity theft and fraud;

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

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

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

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future

[6] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited July 25, 2025).

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;

g. Delay in receipt of tax refund monies;

h. Unauthorized use of stolen PII; and

i. 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.

Significant Risk of Continued Identity Theft

75. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

76. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

77. 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 "[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." *Id.*

78. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the dark web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

79. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[7] Criminals in particular favour the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[8] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

80. The unencrypted PII of Plaintiff and Class Members has or will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

81. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

82. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researchis Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your

[7] *What Is the Dark Web?* EXPERIAN, available at https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited July 25, 2025).
[8] *Id.*

name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[9]

83. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

84. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[10]

85. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

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

[9] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[10] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

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

88. Identity thieves can also use an individual's personal data and PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[11]

89. One example of criminals piecing together bits and pieces of compromised PII to create comprehensive dossiers on individuals is called "Fullz" packages.[12] These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-

[11] *Identity Theft and Your Social Security Number,* SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited July 25, 2025).

[12] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm,* KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited July 25, 2025).

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. For example, they can combine the stolen PII, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

90. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet. 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 highis price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

91. 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.[13]

92. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[14] Yet, Defendant failed to rapidly report to Plaintiff and the Class that their PII was stolen. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class

[13] *2019 Internet Crime Report* (Feb. 11, 2020) FBI.GOV, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited July 25, 2025).
[14] *Id.*

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.

93. 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.

94. 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.

95. 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, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

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

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

97. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding

data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record.

98. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

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

100. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[15]

101. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of PII

102. Personal data like PII is a valuable property right.[16]

[15] *See Federal Trade Commission*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited July 25, 2025).

[16] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII/PHI") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII/PHI, which

103. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

104. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[17]

105. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.

106. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21] According to a report released by the Federal Bureau of

companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (last visited July 25, 2025).

[17] *Shadowy data brokers make the most of their invisibility cloak* (Nov. 5, 2019) LA TIMES, https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 25, 2025).

[18] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/. (last visited July 25, 2025).

[19] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 25, 2025).

[20] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited July 25, 2025).

[21] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 25, 2025).

Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[22]

107. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[23] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.[24]

108. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

109. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

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

110. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

111. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—

[22] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited July 25, 2025).
[23] *The Personal Data Revolutaion,* DATA COUP, https://datacoup.com/ *and How it Works,* DIGI.ME, https://digi.me/what-is-digime/ (last visited July 25, 2025).
[24] *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited July 25, 2025).

e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

112. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

113. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[25]

114. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

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

[25] Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds,* FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited July 25, 2025).

Lost Benefit of the Bargain

117. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

118. When agreeing to provide their PII Wheeling Jesuit University, Plaintiff and Class Members, as clients, understood and expected that they were, in part, paying for services and data security to protect the PII they were required to provide. Likewise, in providing the PII of its alumni to Defendant, Wheeling Jesuit University expected Defendant to maintain client-confidentiality and protect the PII entrusted to it.

119. Plaintiff values data security.

120. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[26] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[27]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[28]

[26] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited July 25, 2025).
[27] *Id*. at 3.
[28] *Id*.

c. 89% of consumers stated that "I care about data privacy."[29]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[30]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[31]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[32]

Defendant Could Have Prevented the Data Breach

121. Data breaches are preventable.[33] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[34] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[35]

122. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [36]

---

[29] *Id*. at 9.
[30] *Id*.
[31] *Id*.
[32] *Id*. at 11.
[33] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[34] *Id.* at 17.
[35] *Id.* at 28.
[36] *Id.*

123. In a Data Breach like the one here, many failures laid the groundwork for the Breach.

124. For example, the FTC has published guidelines that establish reasonable data security practices for businesses. The guidelines also emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

125. Additionally, several industry-standard best practices have been identified that—at a minimum—should be implemented by businesses like Defendant.

Defendant Failed to Adhere to FTC Guidelines

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

127. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

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

131. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to clients' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

132. Experts studying cyber security routinely identify corporations as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

133. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

135. Moreover, companies should retain personal data only as necessary, with legal justification. Personal data should not be stored beyond the time necessary to achieve its initial purpose of collection. In line with industry standard practices, Defendant should have promptly deleted the data belonging to clients.

136. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

137. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

138. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach of Eckert Seaman's network, including all those individuals who received notice of the breach.

139. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

140. Plaintiff reserves the right to amend the class definition.

141. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

142. This action satisfies the numerosity, commonality, typicality, and adequacy requirements.

143. **Numerosity.** The Class members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 9,400members.

144. **Commonality and Predominance.** Plaintiff's and the Class Members' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if 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. if Defendant was negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

145. **Typicality.** Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

146. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

147. **Appropriateness.** The likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case.

Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

148. **Ascertainability.** All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some victims and sent them data breach notices.

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

149. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

150. Plaintiff and the Class entrusted their PII to their agent, Defendant's client, on the premise and with the understanding that their agent/Defendant's client would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

151. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to use adequate data security in accordance with industry standards for data security would compromise the PII of its clients in a data breach. And here, that foreseeable danger came to pass.

152. Defendant's duty of care is an independent, non-contractual duty of care arising from the special relationship between Defendant and Plaintiff, and the fact Defendant assume responsibility to collect and store Plaintiff and the Class Member's PII.

153. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

154. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class Members' PII.

155. Defendant owed—to Plaintiff and Class Members—at least the following duties:

a. To exercise reasonable care in handling and using the PII in its care and custody by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII;

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

c. to prevent unauthorized access to Plaintiff and Class members PII;

d. to detect, in a timely manner, that Plaintiff's and Class members' PII had been compromised; and

e. to remove former clients' PII it was no longer required to retain pursuant to regulations from its systems, including Plaintiff's.

156. Plaintiff and Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

157. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

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

159. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff's agent and the Class. That special relationship arose because the agent of Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of receiving legal services Defendant.

160. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

161. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and Class Members' and the importance of exercising reasonable care in handling it.

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

163. Defendant breached these duties as evidenced by the Data Breach.

164. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff 'and Class Members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

165. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

166. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

167. Defendant has admitted that the PII of Plaintiff and the Class was accessed by an intruder to its systems.

168. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

169. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

170. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

171. 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. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA intended to guard against. Defendant violated Section 5 of the FTCA by failing to adequately safeguard Plaintiff's and Class members' PII.

172. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

173. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

174. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because 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 members of the Class.

175. Defendant's duty to use reasonable security measures also arose under the confidential attorney-client relationship it had with Wheeling Jesuit University, under which Defendant was required to protect the security, confidentiality, and integrity of Wheeling Jesuit University alumni PII. The harm occurring as a result of the Data Breach is the type of harm that the confidential attorney-client relationship intends to guard against. Defendant violated the confidential attorney-client relationship by failing to adequately safeguard Plaintiff's and Class members' PII.

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

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

178. Defendant's violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

179. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

180. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

181. Defendant offered to provide services to Plaintiff, Plaintiff's agent and members of the Class if, and in exchange, the agent of Plaintiff and members of the Class provided Defendant with their PII.

182. In providing their PII, Plaintiff and Class members entered into an implied contract with Defendant, whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class members' PII.

183. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for legal services.

184. Implicit in the agreement between Plaintiff and Class members and the 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.

185. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

186. Defendant accepted possession of Plaintiff's and Class members' PII.

187. Had Defendant disclosed to Plaintiff and Class members that Defendant did not have adequate computer systems and security practices to secure consumers' PII, Plaintiff and Class members would not have provided their PII to Defendant.

188. Defendant recognized that consumers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class

members.

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

190. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusions into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

191. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff's and Class members were deprived of the data protection and security that Defendant promised when Plaintiff

and the Class members entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class members' PII.

192. Additionally, the covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

193. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

194. Defendant failed to send Notice to the victims promptly and sufficiently.

195. In these and other ways, Defendant violated its duty of good faith and fair dealing.

196. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

197. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

198. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

199. This claim is pleaded in the alternative to the breach of implied contract claim.

200. Upon information and belief, Defendant funds its data security measures from its general revenue, including the money generated from Plaintiff's and the Class Members' PII, and payments made by or on behalf of Plaintiff and the Class Members.

201. As such, a portion of the revenue gleaned from Plaintiff's and the Class Members' PII, and a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

202. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they either provided services, in the form of employment, or purchased services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII. In exchange, Plaintiff and Class Members should have had their PII protected with adequate data security.

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

204. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiff and the Class 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.

205. 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.

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

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

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

209. 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) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (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 the Class.

210. 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.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

211. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

212. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

213. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

214. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person. It constitutes an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

215. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class members disclosed their sensitive and confidential information to Defendant as part of seeking Defendant's services, or in the process of obtaining employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

216. The Data Breach constitutes an intentional interference with Plaintiff's and the Class members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

217. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

218. Defendant acted with a knowing state of mind when it failed to notify Plaintiff's and the Class members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

219. Defendant had notice and knew or should have known that its inadequate cybersecurity practices would cause injury to Plaintiff's and the Class members.

220. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

221. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

222. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

223. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their PII. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

224. Plaintiff and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

225. Plaintiff and Class Members seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

226. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

227. Given the relationship between Defendant and Plaintiff and the Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff and Class Members of the Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

228. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

229. Because of the highly sensitive nature of the PII, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

230. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

231. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach within a reasonable and practicable time period.

232. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

233. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

234. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

235. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

236. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant's breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

237. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

238. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences another data breach.

239. And if another breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

240. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

241. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class, and naming Plaintiff as representatives of the Class, and Plaintiff's attorneys as Class Counsel;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the putative Class, demands a trial by jury on all claims so triable.

Dated: August 4, 2025

By: */s/ Jacob U. Ginsburg*
Jacob U. Ginsburg, Esq.
Kimmel & Silverman, PC
30 E. Butler Ave.
Ambler, PA 19002
Direct line: (267) 468-5374
jginsburg@creditlaw.com

Raina C. Borrelli (*pro hac vice* anticipated)
STRAUSS BORRELLI, PLLC
980 N. Michigan Ave., Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
croman@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class