UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

CINDY MENCH, on behalf of herself and all others similarly situated, Plaintiff, v. **MCCORMICK & PRIORE P.C.,** Defendant.	Case No. **PROPOSED CLASS ACTION** **DEMAND FOR JURY TRIAL**

Cindy Mench ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against McCormick & Priore P.C., ("McCormick & Priore" 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 McCormick & Priore's failure to protect the highly sensitive data of its employees, clients, and client's customers. McCormick & Priore's data breach also affects consumers who had no relationship with McCormick & Priore, never sought one, and never consented to McCormick & Priore collecting and storing their information.

2. On December 9, 2024, McCormick & Priore discovered "suspicious activity" on its computer network. By that point, the cybercriminal group Interlock had accessed McCormick & Priore's network from December 6, 2024 to December 9, 2024, and downloaded 3,150 GB of data, amounting to 2,342,500 files and 157,185 folders of private, confidential data.

3. McCormick & Priore has not publicly disclosed who was impacted (*e.g.,* current employees, former employees, clients, etc.) or the complete categories of information

compromised in the Data Breach. However, based on the Notice Plaintiff received, at minimum names, driver's license numbers, and Social Security numbers were stolen. Plaintiff refers to the stolen sensitive information "PII."

4. On or about May 30, 2025 – 175 days after the Data Breach first occurred – McCormick & Priore finally began notifying some Class Members about the Data Breach. The Notice located on the website of the Vermont Attorney General's Office is attached as Exhibit A. Plaintiff's Notice is also dated May 30, 2025.

5. Upon information and belief, cybercriminals were able to breach Defendant's systems 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.

6. Defendant's Notice obfuscates the nature of the Data Breach and the threat it posed. The Notice failed to disclose the identity of the cybercriminals who perpetrated this Data Breach (Interlock), how much data was stolen, many people were impacted, the categories of information acquired, who was impacted (*e.g.*, employees or clients or both), the root cause of the Data Breach happened, why it took Defendant three to four days to detect "suspicious activity," and why Defendant waited 175 days before notifying victims that cybercriminals had gained access to their highly private information.

7. 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.

8. 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.

9. In failing to adequately protect the sensitive information of its employees, clients, and client's customers, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its employees, clients, and client's customers.

10. Plaintiff and the Class are victims of Defendant's negligence and inadequate cybersecurity measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust when Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Cindy Mench is a victim of the Data Breach. Her name, Social Security number, and driver's license number were exposed during the Data Breach.

12. 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.

13. Plaintiff seeks on behalf of herself and the Class monetary damages and injunctive relief including lifetime credit monitoring and ID theft monitoring.

PARTIES

14. Plaintiff, Cindy Mench is a natural person and citizen of Quakertown, PA, located in Bucks County, where she intends to remain.

15. Defendant McCormick & Priore, P.C., is professional corporation with its headquarters and principal place of business located at 2001 Market Street, Suite 3810, Philadelphia, PA 19103. It also has offices in Plymouth Meeting, PA, and Princeton, NJ.

JURISDICTION AND VENUE

16. 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, including at least Massachusetts and Vermont, and there are over 100 putative Class members.

17. This Court has personal jurisdiction over Defendant because it maintains its headquarters and principal place of business in this District, regularly conducts business Philadelphia, Pennsylvania, and has sufficient minimum contacts in Philadelphia, Pennsylvania.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1)–(d) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

19. McCormick & Priore is a law firm based in Pennsylvania. Founded in 1994, McCormick & Priore represents the interests of clients in a wide range of industries, offering expertise in defense litigation for insurance-related companies as well as manufacturers.[1] McCormick & Priore serves a wide range of clients, from multinational corporations to mid-size companies as well as individuals.[2] Headquartered in Philadelphia, Pennsylvania, McCormick & Priore has additional locations in Pennsylvania, New Jersey, New York, and Delaware.[3]

20. On information and belief, McCormick & Priore accumulates highly private PII of

[1] *Home,* MCCORMICK & PRIORE, https://mccormickpriore.com/ (last visited June 9, 2025); *Practice Areas,* MCCORMICK & PRIORE, https://mccormickpriore.com/ (last visited June 9, 2025).
[2] *Id.*
[3] *Our Offices,* MCCORMICK & PRIORE, https://mccormickpriore.com/ (last visited June 9, 2025).

its employees, clients, and clients' customers. For example, McCormick & Priore represents insurance carriers "on all aspects of coverage issues, arising from virtually any setting." In representing insurance carriers, McCormick & Priore obtained the PII of its clients' customers. Given its age, McCormick & Priore has accrued approximately 30 years of data and contracts.

21. In collecting and maintaining the PII of its employees, clients, and clients' customers, McCormick & Priore 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.

22. McCormick & Priore, a law-firm which claims "trustworthiness" is one of the qualities it values most, understood the need to protect the PII of its employees, clients, and clients' customers, and prioritize its data security.

23. Indeed, McCormick & Priore offers mediation and arbitration services, which are supposedly confidential, and recently hosted a podcast on the intersection between law, technology, and forensic science.

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

Defendant Failed to Safeguard the PII of Plaintiff and the Class

25. Plaintiff is a customer of Erie Insurance Exchange. Upon information and belief, McCormick & Priore provides legal assistance and counsel to Erie Insurance Exchange, and

thorough this relationship, obtained Plaintiff's PII.

26. Plaintiff received Defendant's Notice on the first week of June 2025, informing her that her PII was compromised, including her name, driver's license number, and Social Security number. Plaintiff does not understand why McCormick & Priore needed Plaintiff's PII to provide legal advice to her insurance company.

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

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

29. On December 9, 2024, Defendant became aware cybercriminals hacked its network and "may have" downloaded files containing extremely sensitive information, including Social Security numbers.

30. Defendant did not disclose how many people were impacted, but, upon information and belief, at least residents in Vermont, Pennsylvania, and Massachusetts were impacted.

31. The Data Breach shows Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of the highly private information employees, clients, and clients' customers, for a period of four days.

32. On or about May 30, 2025 – 175 days after the Data Breach first occurred – Defendant finally began notifying some Class Members the Data Breach. Ex. A.

33. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

34. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing the PII of its employees, clients, and client's customers, as evidenced by the Data Breach.

35. 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. To the extent Defendant actually needed the PII of its clients' customers to render legal advice to its clients, it should have promptly deleted the PII of its clients' customers after it provided its clients with advice and/or representation.

36. In response to the Data Breach, Defendant contends "we have taken steps to further enhance our existing cybersecurity infrastructure, as well as implemented additional policies and procedures to minimize the reoccurrence of future similar events." Ex. A. Although Defendant fails to expand on what these "policies and procedures" are in any detail, such "policies and procedures" if implemented at all, should have been in place before the Data Breach.

37. Through its Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors." Ex. A.

38. Despite advising its employees, clients, and client's customers to remain vigilant, Defendant waited an unreasonable amount of time before it began notifying victims, depriving 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.

39. On information and belief, Defendant has offered complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face

following the Data Breach. Indeed, the information compromised involves PII that cannot be changed, such as Social Security numbers.

40. Even with several months 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 (although in Plaintiff's case, her Social Security number was compromised). 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 the PII of employees, clients, and client's customers. Defendant's negligence is evidenced by its failure to prevent the Data Breach, to detect the Data Breach for at least three days, and to stop cybercriminals from accessing the PII it stored in its network.

43. Furthermore, Defendant's Notice obfuscates the nature of the Data Breach and the threat it posed. The Notice failed to disclose the identity of the cybercriminals who perpetrated this Data Breach (Interlock), how much data was stolen, many people were impacted, the categories of information acquired, who was impacted (*e.g.*, employees or clients or both), the root cause of the Data Breach happened, why it took Defendant three to four days to detect "suspicious

activity," and why Defendant waited 175 days before notifying victims that cybercriminals had gained access to their highly private information.

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. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

45. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiffs' and Class Members' Social Security numbers for download and theft.

46. In the context of notice of data breach letters of this type, Defendant's use of the phrase "may have accessed or downloaded" is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese – by sending a notice of data breach letter to Plaintiff and Class Members, it admits that Defendant itself has a reasonable belief that Plaintiff's and Class Members' names, Social Security numbers, and other sensitive information were accessed or acquired by an unknown actor – aka cybercriminals.

47. Moreover, in its Notice, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and downloaded 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.

Interlock Ransomware Obtained the PII of Plaintiff and the Class and Posted it for Sale

48. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class Members' PII for theft and sale on the Dark Web.

49. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII appear to be the notorious cybercriminal group Interlock Ransomware.[4]

50. Interlock Ransomware first emerged in September 2024 and quickly developed a reputation for targeting high-value sectors.[5] Interlock's methods closely follow widely recognized cyberattack patterns, using a range of techniques to infiltrate and maintain control over targeted systems.[6] The group typically gains access by stealing login credentials, exploiting security flaws in public-facing applications, or tricking users into downloading malware through deceptive links and fake updates.[7] Once inside, they execute malicious code using scripting tools and disguised installers.[8]

51. When a company is impacted, it will find that its files have not only been encrypted but have also had ".interlock" appended to their filenames.[9] For example, a file named report.xlsx

---

[4] *Victims*, RANSOMWARE LIVE, https://www.ransomware.live/id/Q29tbXVuaXR5IEhvc3BpdGFsIG9mIEFuYWNvbmRhQG1lb3c= (last visited May 25, 2025).
[5] Joel Francis, *Briefing 34: Beyond the Breach: Assessing Downstream Risk from Interlock Ransomware* (June 3, 2025), KRATOS, https://www.kratosdefense.com/constellations/articles/ransomware-attack-by-interlock-targets-national-defense-corporation (last visited June 9, 2025).
[6] *Threat Actor Profile: Interlock Ransomware Group* (May 6, 2025), CYBLE, https://cyble.com/threat-actor-profiles/interlock-ransomware-group/ (last visited June 9, 2025).
[7] *Id.*
[8] *Id.*
[9] *Supra,* note 5.

would become report.xlsx.interlock, visibly signaling that it has been encrypted by Interlock.[10] Following the encryption, Interlock steals the data, leveraging a double extortion strategy to coerce payments from victims.[11]

52. While many elements of Interlock's behavior point to financially motivated cybercrime, its choice of target and the strategic value of the exfiltrated data suggest broader implications.[12] For example, on its Dedicated Leak Site, Interlock states the following:

> We are INTERLOCK, a relentless collective that exposes the recklessness of companies failing to protect their most crucial assets: customer data and intellectual property. We exploit the vulnerability they leave wide open, deliver a harsh but necessary wake-up call to those who think they can cut corners on security.
> …
> We don't just want payment; we want accountability. Our actions send a message to those who hide behind weak defenses and half-measures: your data is only as safe as the effort you put into protecting it. If you don't take data security seriously, we will on your behalf. Pay attention or pay the price. In this digital age, there's no excuse for complacency. When companies neglect cybersecurity, we make them pay not just with ransoms, but with lessons they won't forget. We are here to enforce the standards they fail to uphold.

53. This message, which Interlock posted on its Dark Leak Site, is posted below:[13]

[10] *Id.*
[11] *Supra,* note 6.
[12] *Supra,* note 5.
[13] *Id.*

54. On or around December 25, 2024, Interlock claimed credit for the Data Breach in a post on its Dark Leak Site.[14]

55. On its Dedicated Leak Site, Interlock bragged that it had stolen large collection of SQL databases, or Structured Query Language databases, from McCormick & Priore.[15] SQL databases contain vast amounts of information. For example, a SQL database used for customer service can have one table for customer names and addresses and other tables that hold information about specific purchases, product codes and customer contacts.[16]

56. Moreover, on or around December 25, 2024, Interlock claimed to have stolen an outstanding **3,150 GB of data,** 2,342,500 files, and 157,185 folders. One Gigabyte is equivalent to 1000 megabytes, and the entire written works of Shakespeare could fit inside of just 5 megabytes.[17] Therefore, it is likely that the Data Breach impacted the confidential data of tens of thousands of individuals.

57. Moreover, if McCormick & Priore first detected "suspicious activity" on December 9, 2024, and Interlock posted the data on or around December 25, 2025, Interlock gave McCormick & Priore approximately two weeks to pay the ransom. Upon information and belief, McCormick & Priore did not pay the ransom, because the stolen data was available for download and purchase via the button "GET."

---

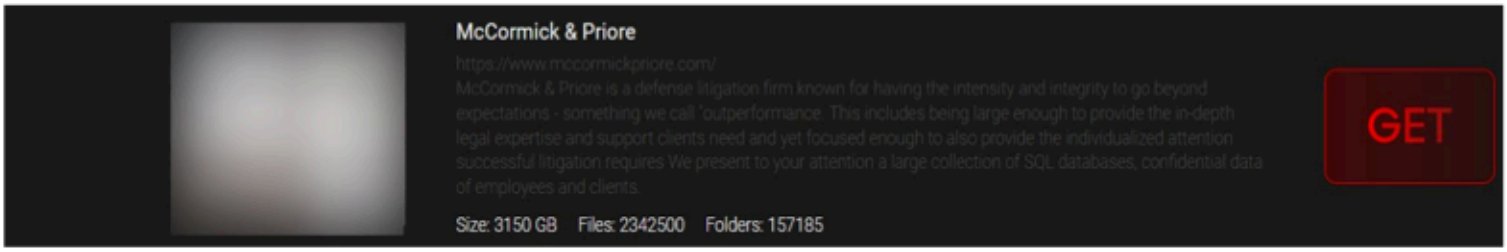
[14] *McCormick & Priore*, RANSOMLOOK, https://www.ransomlook.io/search, and *Hack Tuesday Week 25 – 31 December 2024,* HACKMANAC, https://hackmanac.com/news/hack-tuesday-week-25-31-december-2024 (last visited June 9, 2025).

[15] *McCormick & Priore*, RANSOMLOOK, https://www.ransomlook.io/search, and *FalconFeeds - McCormick & Priore P.C.,* TWITTER, https://x.com/FalconFeedsio/status/1871986777696915790/photo/1 (last visited June 9, 2025).

[16] Kinza Yasar, *What is Structured Query Language (SQL)?* (Aug. 27, 2024), TECHTARGET, https://www.techtarget.com/searchdatamanagement/definition/SQL#:~:text=For%20example%2C%20a%20SQL%20database,product%20codes%20and%20customer%20contacts (last visited June 9, 2025).

[17] Paulette Keheley, *How Many Documents in a Gigabyte?* (April 2, 2020), DWR EDISCOVERY, https://www.digitalwarroom.com/blog/how-many-pages-in-a-gigabyte (last visited June 9, 2025).

58. A copy of the description of Interlock Ransomware's post to its Dedicated Leak Site is posted below:[18]



59. Thus, on information and belief, Interlock has ***already sold or leaked*** the stolen PII of tens of thousands of Defendant's employees, clients, and client's customers.

60. Thus, on information and belief, Plaintiff's and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

61. Moreover, Interlock claims, and the data it leaked also suggests, that it successfully stole data from McCormick & Priore. Yet McCormick & Priore intentionally obfuscates the nature of the breach, instead claiming that an unauthorized third party *may have* accessed or downloaded files – when it knew all along that Interlock Ransomware did in fact acquire its client's data, and demanded a ransom for it.

62. Therefore, upon information and belief, McCormick & Priore's Notice to Plaintiff and the Class is false, intentionally misleading, and intentionally downplays the severity of the Data Breach and the threat it poses to its employees, clients, and client's customers.

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

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

[18] *FalconFeeds - McCormick & Priore P.C.*, TWITTER, https://x.com/FalconFeedsio/status/1871986777696915790/photo/1 (last visited June 9, 2025).

64. Defendant's data security obligations were particularly important given its status as a fiduciary of its clients' data, and the substantial increase in cyberattacks and/or data breaches in recent years. In light of past high profile data breaches at industry-leading companies, including, for example, 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), Defendant knew or, if acting as a reasonable business, should have known that the PII it collected and maintained would be vulnerable to and targeted by cybercriminals.

65. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[19]

66. 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."[20]

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

68. 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

---

[19] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited June 9, 2025).

[20] 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 June 9, 2025).

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.

69. 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.

70. 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

71. Plaintiff is a data breach victim, having received Notice the first week of June 2025.

72. On information and belief, Defendant obtained Plaintiff's PII from her insurance company. As a condition of receiving services to Plaintiff's insurance company, Defendant required Plaintiff's PII, including at least her name, driver's license number, and Social Security number.

73. Plaintiff is unsure why Defendant needed her PII to provide legal advice to her insurance company, and why Defendant did not delete her data after it no longer had any use for it, or any legal justification to maintain it.

74. 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.

75. Importantly, Plaintiff does not recall ever learning that her PII was compromised in former a data breach incident, other than the breach at issue in this case.

76. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Data Breach.

77. Plaintiff suffered actual injury from the exposure of her PII —which violates her rights to privacy. Following the Data Breach, Bank of America notified Plaintiff by email that her private information had been published on the Dark Web. Therefore, upon information and belief, Plaintiff's PII is already in the hands of cybercriminals.

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

79. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit information.

80. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft, just as Defendant directed her to do in its Notice.

81. Plaintiff fears for her personal financial security. 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 her 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.

82. Following the Data Breach, Plaintiff discovered someone opened up a post office box under her name. Therefore, Plaintiff is already the victim of identity theft, as 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). 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.* Therefore, fraudulently opening a post office boxc in one's nam e is a form of identity theft because it involves using the personal information of the victim, to impersonate him or her, and gain access to their mail.

83. Here, the fraudsters successfully used Plaintiff's PII to open up a post office box and receive mail in her name, thereby enable the fraudster to receive mail intended for Plaintiff. The address, and the mail received at the address, could then be used to perpetrate additional forms of identity theft, such as financial fraud, synthetic identity theft, and brushing scams.

84. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

85. Once an individual's PII is for sale and accessible on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[21] Plaintiff's name, address, and Social Security number were compromised as a result of the Data Breach, and upon information and belief, have been published and sold on the Dark Web.

[21] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited June 9, 2025).

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

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

87. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' PII directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their PII in the Data Breach.

88. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, inter alia, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. identity theft and fraud;

b. loss of time to mitigate the risk of identity theft and fraud;

c. diminution in value of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud;

e. lost benefit of the bargain and opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, inter alia, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

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

h. compromise and continuing publication of their PII;

i. unauthorized use of their stolen PII;

j. invasion of privacy; and

k. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

Significant Risk of Continued Identity Theft

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

90. 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).

91. 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.*

92. 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.

93. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[22] 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

[22] *What Is the Dark Web?* EXPERIAN, available at https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited June 9, 2025).

the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[23] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

94. 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.

95. The value of Plaintiff's and Class's PII on the black market is considerable. Stolen PII trades on the black market for years and is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

96. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

97. 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.

98. 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

[23] *Id.*

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.

99. 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.[24]

100. One example of criminals piecing together bits and pieces of compromised PII to create comprehensive dossiers on individuals is called "Fullz" packages.[25] These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers

---

[24] *Identity Theft and Your Social Security Number,* SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited June 9, 2025).

[25] "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 June 9, 2025).

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.).

101. 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 higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

102. 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.[26]

103. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[27] 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 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.

---

[26] *2019 Internet Crime Report* (Feb. 11, 2020) FBI.GOV, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited June 9, 2025).
[27] *Id.*

104. 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.

105. 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.

106. 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

107. 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.

108. Plaintiff has already experienced identity theft. In the event that Plaintiff and Class Members experience further 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.

109. 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.

110. 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.

111. 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.[28]

112. 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

113. Personal data like PII is a valuable property right.[29]

---

[28] *See Federal Trade Commission*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited June 9, 2025).

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

114. 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.

115. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[30]

116. 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.[31] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.[32]

117. 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.

118. 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

119. 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.

---

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 June 9, 2025).

[30] *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 June 9, 2025).

[31] *The Personal Data Revolutaion,* DATA COUP, https://datacoup.com/ *and How it Works,* DIGI.ME, https://digi.me/what-is-digime/ (last visited June 9, 2025).

[32] *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited June 9, 2025).

120. 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—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.

121. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her 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.

122. 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.[33]

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

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

125. 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

[33] 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 June 9, 2025).

minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Lost Benefit of the Bargain

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

127. When agreeing to provide their PII, which was a condition precedent to obtain services or employment from Defendant, Plaintiff and Class Members, as employees, clients, and client's customers, understood and expected that they were, in part, paying for services and data security to protect the PII they were required to provide.

128. Plaintiff values data security. Indeed, data security is an important consideration of seeking an insurance carrier, employment, or legal services.

129. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[34] 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."[35]

[34] *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 June 9, 2025).
[35] *Id.* at 3.

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."[36]

c. 89% of consumers stated that "I care about data privacy."[37]

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.[38]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[39]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[40]

130. Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant and/or their third party agents.

Defendant Could Have Prevented the Data Breach

131. Data breaches are preventable.[41] 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."[42] She added that "[o]rganizations that collect, use, store, and share sensitive personal

[36] *Id.*
[37] *Id.* at 9.
[38] *Id.*
[39] *Id.*
[40] *Id.* at 11.
[41] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[42] *Id.* at 17.

data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[43]

132. "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." [44]

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

134. 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.

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

136. Defendant could have prevented this Data Breach by properly training personnel, securing account access through measures like phishing-resistant (i.e., non-SMS text based) multifactor authentication ("MFA") for as many services as possible, training users to recognize and report phishing attempts, implementing recurring forced password resets, and/or securing and encrypting files and file servers containing Plaintiff's and Class Members' PII, but failed to do so.

137. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' PII, using controls like limitations on personnel with access to sensitive data and requiring phishing-resistant MFA

[43] *Id.* at 28.
[44] *Id.*

for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access. Defendant would have recognized the malicious activities if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

Defendant Failed to Adhere to FTC Guidelines

138. 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.

139. 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.

140. 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.

141. 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.

142. 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.

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

Defendant Failed to Follow Industry Standards

144. Experts studying cybersecurity routinely identify financial corporations as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

145. 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.

146. 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.

147. 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 employees, clients, and client's customers.

148. 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 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

149. 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

150. 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 McCormick & Priore's network, including all those individuals who received notice of the breach.**

151. 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.

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

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

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

155. **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 9,667 members.

156. **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 stored PII beyond the time necessary to achieve its initial purpose of collection, should have promptly deleted the data belonging to the victims;

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

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

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

g. if Defendant's Breach Notice was reasonable;

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

i. what the proper damages measure is; and

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

157. **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.

158. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's common interests. her 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.

159. **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.

160. **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)

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

162. Defendant solicited, gathered, and stored the PII of Plaintiffs and the Class.

163. Plaintiff and the Class, or their third party agents, entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

164. 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 their PII in a data breach. And here, that foreseeable danger came to pass.

165. 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.

166. 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.

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

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

168. 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.

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

170. 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.

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

172. 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.

173. 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.

174. 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.

175. Defendant breached these duties as evidenced by the first and second Data Breach.

176. 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.

177. 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.

178. Defendant further breached its duties by failing to provide a reasonable and 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.

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

180. 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.

181. 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)

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

183. Defendant's violation of its statutory duties, including those outlined in the FTC Act, the Pennsylvania Consumer Data Privacy Act and the Breach of Personal Information Notification Law, were a substantial factor in bringing about Plaintiff's harm. The FTC Act is designed to protect consumers, including Plaintiff and the Class Members, and promote fair competition

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

185. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

186. 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.

187. 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.

188. Defendant had a duty to Plaintiff and the members of the Classes to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Classes' PII.

189. Defendant breached its respective duties to Plaintiff and members of the Classes under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Classes' PII.

190. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

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

192. 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.

193. Had Plaintiff and members of the Classes known that Defendant did not adequately protect their PII, Plaintiff and members of the Classes would not have entrusted Defendant, or their third-party agents, with their PII.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 Contract
(On Behalf of Plaintiff and the Class)

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

195. Defendant entered into various contracts with its clients, including corporations and insurance carriers, to provide services to its clients.

196. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, Plaintiff and the Class are third-party beneficiaries of the contract and have the right to enforce the contract's provisions. Indeed, considering the nature of the services McCormick & Priore provides to its clients, the direct and primary objective

of the contracting parties includes the collection and protection of the PII belonging to Plaintiff and the Class, for their benefit.

197. Defendant knew that if it were to breach these contracts with its insurance provider clients, the clients' customers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

198. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

199. It is just and practical to permit Plaintiff, for whose benefit the contract between his insurance carrier and McCormick & Priore was made, to enforce it against McCormick & Priore.

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

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

201. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into an implied breach of contract for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

202. For example, Defendant offered to provide employment and/or services to Plaintiff and members of the Class if, and in exchange, Plaintiff and members of the Class provided Defendant with their PII. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized persons.

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

204. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with reasonable, prompt, and adequate notice of all unauthorized access and/or theft of their PII.

205. Plaintiff and the members of the Class would not have entrusted their PII to Defendant, or their third party agents, in the absence of such an agreement with Defendant.

206. 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;

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

d. Failing to delete the PII of Plaintiffs and Class Members once Defendant no longer had a reasonable need to maintain it.

207. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

208. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

209. 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.

210. 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.

211. Defendant failed to send adequate Notice to the victims promptly.

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

213. 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.

214. Plaintiff, on behalf of herself 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.

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

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

216. the third-party agents provided valuable PII to Defendant, in exchange for services.

217. Upon information and belief, Defendant funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

218. As such, 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.

219. Plaintiff and Class Members conferred a monetary benefit on Defendant in providing PII to their third-party agents, who entered into contracts with Defendant whereby the third-party agents provided valuable PII to Defendant, in exchange for services. Other Class Members provided services, in the form of employment, or purchased legal 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 received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

220. 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, as the receipt of Plaintiff's and the Class's PII was used to facilitate its services to Plaintiff and the Class.

221. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

222. 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.

223. 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.

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

225. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant either directly or through their insurance carriers.

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

227. 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.

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

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

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

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

231. 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 by applicable laws set forth herein, including but not limited to, state and federal privacy and consumer protection statutes, common law, and Pennsylvania law including the Pennsylvania Consumer Data Privacy Act and the Breach of Personal Information Notification Law.

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

233. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiff and the Class to provide and store on its own servers constitutes a violation Plaintiff and the Class's right to privacy.

234. 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.

235. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII 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.

236. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

237. Defendant knowingly did not notify Plaintiff's and Class Members in a timely fashion about the Data Breach.

238. 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.

239. 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 as set forth *supra*.

240. 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.

241. 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.

242. 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.

243. 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.

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

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

245. Given the relationship between Defendant on the one hand, and the third-party agent of Plaintiff and the Class Members on the other hand, 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.

246. Defendant, as a provider of legal services, 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.

247. Because of the highly sensitive nature of the PII, Plaintiff and Class Memebers would not have entrusted Defendant (or their third-party agents), or anyone in Defendant's

position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

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

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

250. 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 including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

251. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses (as detailed *supra*).

EIGHTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

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

253. Plaintiff and class members have an interest, both equitable and legal, in the Personal Information about them that was conveyed or provided to, collected by, and maintained by Defendant, and that was ultimately accessed or compromised in the Data Breach.

254. As a provider of legal services, Defendant has a special relationship to its clients and other affiliated persons, like Plaintiff and the class members.

255. Because of that special relationship, Defendant were provided with and stored private and valuable PHI and other Personal Information related to Plaintiff and the class, which it was required to maintain in confidence.

256. Plaintiff and the class provided Defendant with their Personal Information under both the express and/or implied agreement of Defendant to limit the use and disclosure of such information.

257. Defendant owed a duty to Plaintiff and the class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

258. Defendant had an obligation to maintain the confidentiality of Plaintiff's and the class members' Personal Information. Plaintiff and the class have a privacy interest in their personal legal matters, and Defendant had a duty not to disclose confidential legal information and PII concerning its employees, clients, and client's customers.

259. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Personal Information and confidential legal information of Plaintiff and the class.

260. Plaintiff and the class's Personal Information is not generally known to the public and is confidential by nature.

261. Plaintiff and class members did not consent to nor authorize Defendant to release or disclose their Personal Information to an unknown threat actor.

262. Defendant breached the duties of confidence it owed to Plaintiff and the class when Plaintiff's and class members' Personal Information was disclosed to unknown and unauthorized parties.

263. Defendant breached its duties of confidence by failing to safeguard Personal Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) designing and implementing inadequate cybersecurity safeguards and controls; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PII and legal information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the class members' Personal Information to a criminal third party.

264. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiff and the class members, their privacy, confidences, and Personal Information would not have been compromised.

265. As a direct and proximate result of Defendant's breach of confidences, Plaintiff and the class have suffered and/or are at a substantial increased risk of suffering injuries, including:

a. The erosion of the essential and confidential relationship between Defendant and Plaintiff and the class as patients;

b. Loss of the privacy and confidential nature of their PII;

c. Theft of their PII;

d. Costs associated with the detection and prevention of identity theft;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Personal Information against theft and not allow access and misuse of data by others;

j. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and the class members' data;

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

266. Additionally, Defendant received payments from Plaintiff and the class members for services with the understanding that Defendant would uphold their responsibilities to maintain the confidences of Plaintiff's and class members' private information.

267. Defendant breached the confidence of Plaintiff and the class members when it made an unauthorized release and disclosure of their Personal Information and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff's and class members' expense.

268. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

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

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

270. 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.

271. 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.

272. 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.

273. 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. Among other things, this should include the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their PII, as well as the steps Defendant's employees should take to protect themselves.

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

275. And if a second 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.

276. 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.

277. 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: June 10, 2025

By: /s/ *Patrick Howard*

Patrick Howard, Esq. (Atty. ID #88572)
SALTZ MONGELUZZI & BENDESKY, PC
1650 Market Street, 52nd Floor
One Liberty Place
Philadelphia, PA 19103
Tel: (215) 496-8282
Fax: (215) 754-4443
Email: phoward@smbb.com

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

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

McCormick & Priore PC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

McCORMICK & PRIORE, P.C.
ATTORNEYS AT LAW
WWW.MCCORMICKPRIORE.COM

P
[redacted]

May 30, 2025

P 0000101102G0400

Dear [redacted],

McCormick & Priore PC is writing to notify you of a recent data event that may affect certain information related to you as described below. McCormick & Priore PC provides legal assistance and counsel for [redacted], and through this relationship and in the normal course of business, McCormick & Priore PC is in possession of a limited amount of information related to you that may have been subject to unauthorized access. This letter includes information about the matter, our response, and resources we are making available to you on behalf of [redacted].

What Happened? On December 9, 2024, we first identified suspicious activity on one legacy system on our network. We promptly conducted an investigation, which included working with third-party specialists to determine the nature and scope of the event. Our investigation identified that as part of the activity, a limited amount of information may have been accessed or downloaded by an unauthorized individual between December 6 and December 9, 2024. After the scope of the unauthorized activity was confirmed, we conducted a diligent review of the relevant information to determine the information contained therein to whom it related to assess potential notification obligations. This comprehensive review was completed on April 25, 2025, after which we promptly notified [redacted] on April 28, 2025 regarding this matter, for necessary approval and contact information for you to issue this notification to you. On May 9, 2025, [redacted] provided the necessary information, we thereafter worked to align resources for notification as quickly as possible.

What Information Was Involved? The types of information related to you that may have affected in connection with this matter include [redacted].

What We Are Doing. In response to this matter, we took steps to secure our environment, and conducted a comprehensive investigation, which was aided by third-party forensic specialists, into the activity. Once the information that may have been impacted was confirmed, we diligently reviewed the information and to whom it related in order to assess potential notification obligations. We also notified federal law enforcement regarding this matter. The obligation to safeguard information in our care is of paramount importance to McCormick & Priore, and in response to this matter we have taken steps to further enhance our existing cybersecurity infrastructure, as well as implemented additional policies and procedures to minimize the reoccurrence of future similar events.

Additionally, out of an abundance of caution, we are offering you access to 24 months of Single Bureau Credit Monitoring and identity protection services through CyberScout, a TransUnion company at no cost to you. Please understand that due to privacy laws, neither McCormick & Priore [redacted] is able to activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is in the "*Steps You Can Take to Help Protect Your Information*" section of the letter below.

What You Can Do. In addition to enrolling in the complimentary monitoring service detailed within, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is recommended that you promptly contact the financial institution or credit/debit card company. You can also review the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional information and resources.

For More Information. We understand that you may have additional questions about this matter. Should you have any questions or concerns regarding this matter or the offered monitoring service, please write to us at 2001 Market Street, Suite 3810, Philadelphia, PA 19103 or contact our dedicated support line at [redacted], available from Monday to Friday, between 8:00 a.m. and 8 p.m. Eastern Time, excluding holidays.

Sincerely,

McCormick & Priore PC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll In Offered Monitoring Services

We are providing you with access to credit monitoring and cyber monitoring services at no charge. To enroll in the monitoring services, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to enroll in the offered monitoring services: [redacted]

Below please find descriptions of offered services we are providing through CyberScout, a TransUnion company.

- Credit Monitoring and Cyber Monitoring
  - Provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. The alert will be sent to you the same day that the change or update takes place with the bureau.
  - Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online.
- Identity Theft Insurance
  - Enrolled individuals will have access to $1,000,000 in insurance coverage to protect against potential damages related to identity theft and fraud.
  - Available worldwide and includes coverage for identity theft expenses as well as unauthorized electronic fund transfer fraud.
- Fraud Remediation Services
  - Access to team of dedicated specialists at CyberScout, a TransUnion company, to help you in the event you experience fraud and assist with remediation.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. McCormick & Priore PC may be contacted at 2001 Market Street, Suite 3810, Philadelphia, PA 19103.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection. McCormick & Priore PC may be contacted at 2001 Market Street, Suite 3810, Philadelphia, PA 19103.

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Cindy Mench

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Patrick Howard - Saltz Mongeluzzi & Bendesky PC
1650 Market St., 52nd Fl., Philadelphia PA 19103

DEFENDANTS

McCormick & Priore P.C.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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)***:
Class Action Fairness Act, 28 USC 1332(d)

Brief description of cause:
DATA BREACH

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

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

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM

Place of Accident, Incident, or Transaction: Bucks County, PA

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

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

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

Civil Litigation Categories

A. Federal Question Cases:

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

B. Diversity Jurisdiction Cases:

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

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

ARBITRATION CERTIFICATION (CHECK ONLY ONE BOX BELOW)

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

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

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

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