UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

CAROLYN GALE, on behalf of herself and all others similarly situated, 1017 Susquehanna Avenue Middle River, MD 21220 Plaintiff, v. KELLY & ASSOCIATES INSURANCE GROUP, INC., dba KELLY BENEFITS, Defendant.	Case No. **JURY TRIAL DEMANDED**

Carolyn Gale through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Kelly & Associates Insurance Group, Inc., dba Kelly Benefits ("Defendant" or "Kelly Benefits"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF THE ACTION

1. This class action arises from Defendant's failure to protect the highly sensitive data of 32,234 individuals.[1] The breach notification Kelly Benefits sent to Maine residents is attached as Exhibit 1.

2. According to Kelly Benefits' breach notice, Kelly Benefits "recently" learned of suspicious activity within its environment. As a result, Defendant launched an investigation to determine the nature of the event. Ex. 1.

[1] *Data Breach Notification, Kelly & Associates Insurance Group, Inc.,* MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/047b774f-2e79-4a04-9f4c-4dd7a8b2ee8d.html (last visited April 21, 2025).

3. Through its investigation, Kelly Benefits confirmed that between December 12, 2024, and December 17, 2024, its "environment was subject to unauthorized access…and certain files were copied and taken." As a result, Kelly Benefits began a review of the data to determine what information had been impacted as well as identify the specific individuals affected, which it completed on March 3, 2025. On or around April 9, 2025, Kelly Benefits began providing written notice of this incident. *Id.*

4. While the information impacted varies depending on the individual, the type of information potentially exposed includes personally identifying information, including names and Social Security numbers, as well as protected health information including information contained with the University of Maryland Medical System (the "Data Breach"). *Id.* Plaintiff refers to the compromised data as "PII/PHI."

5. Kelly Benefits does not disclose how long it took it to discover the ***five-day data breach***. However, Kelly Benefits waited 118 days, from the date of the breach until April 9, 2025, before it finally began notifying Class Members about the Data Breach. *Id.* Defendant failed to post a data breach notice on its website, which is common industry practice.

6. 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/PHI of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI—rendering it an easy target for cybercriminals.

7. The Notice of the Data Breach obfuscates the nature of the Data Breach and the threat it posed. Ex. 1. Indeed, certain files belonging to Plaintiff and the Class were "copied and taken," *i.e., stolen,* by an unauthorized third party over a period of five days. The Notice fails to

disclose who exactly was impacted (employees, clients, employees of clients, etc.), how many people were impacted, how the Data Breach happened including how cybercriminals were able to avoid detection for no less than *five days*, exactly what information was compromised, when Defendant discovered the breach, or why it took the Defendant approximately four months before it finally began notifying some victims that cybercriminals had gained access to their highly private information.

8. Defendant's 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.

9. 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/PHI misuse.

10. In failing to adequately protect the PII/PHI of individuals whose PII/PHI was in Defendant's custody and control, by failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of individuals.

11. Plaintiff and the Class are victims of Defendant's negligence and inadequate cybersecurity measures. Specifically, Plaintiff and members of the proposed Class (or their third-party agents) trusted Defendant with their PII/PHI. But Defendant betrayed that trust when Defendant failed to properly use industry-standard security practices to prevent the Data Breach.

12. Plaintiff is a victim of the Data Breach, and according to the Notice she received on or around April 17, 2025, her name and Social Security number may have been compromised.

13. The exposure of one's PII/PHI 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.

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

PARTIES

15. Plaintiff, Carolyn Gale, is a natural person and citizen of Maryland, residing in Middle River, Maryland, where she intends to remain. Ms. Gale is a Data Breach victim, receiving Notice of the Data Breach on or around April 17, 2025.

16. Defendant Kelly & Associates Insurance Group, Inc., dba Kelly Benefits, is a domestic limited liability company headquartered at 1 Kelly Way, Sparks, Maryland 21152.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one Defendant and Plaintiff are citizens of different states.

18. This Court has personal jurisdiction over Defendant because at least one Defendant maintains its principal place of business in this District and does substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial

part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

20. Kelly Benefits is benefits administration company based in Maryland. Founded in 1976 as Francis X. Kelly Associates, Inc., Kelly Benefits officially became Kelly & Associates Insurance Group, Inc. in 1998. Kelly Benefits' services include consulting, brokerage, and administration services for employee benefits including online benefit administration, consolidated invoices, and compliance oversight programs for employers. In 2007, Kelly Benefits established Kelly Integral Solutions LLC as an umbrella management company for its various facets, including its benefits administration and technology, payroll, and benefits consulting offerings.[2]

21. Given the nature of benefits administration, Defendant accumulates highly private PII/PHI of its employees, clients, and clients' employees.

22. In collecting and maintaining the PII/PHI of its employees, clients, and clients' employees, Defendant 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/PHI.

23. Kelly Benefits understood the need to protect the PII/PHI of employees, clients, and clients' employees, and the need to prioritize its data security. Indeed, Kelly Benefits represented in its privacy policy that:

- "Your privacy, and the privacy of the information provided, is important to us. We use reasonable care to protect your data from loss, misuse, unauthorized access, disclosure, alteration and untimely destruction. We grant access to personal information about you only to our employees, agents, affiliates and

[2] *Our History,* KELLY BENEFITS, https://kellybenefits.com/about/our-history/ (last visited April 21, 2025).

service providers so they can provide you with the necessary online services and support."

- "Please be assured that the Site is equipped with security measures to protect the information you provide us."
- "The personal identifiable information that you provide to us via the Site will not be shared or transferred to unrelated third parties without your prior consent, unless it is required by law or judicial order, or directly related to the services requested."
- "Protecting the privacy of our clients and users of our Site is important."[3]

24. On information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect the PII/PHI of its employees, clients, and clients' employees, or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leave significant vulnerabilities in its systems for cybercriminals to exploit and gain access to the PII of its employees, clients, and clients' employees.

[3] *Privacy Policy,* KELLY BENEFITS, https://kellybenefits.com/privacy-policy/ (last visited April 21, 2025).

Defendant Failed to Safeguard the PII of Plaintiff and the Class

25. Upon information and belief, the Data Breach impacted people all over the United States. Kelly Benefits reported the Data Breach to at least the Attorney Generals of Maine, New Hampshire, South Carolina, Massachusetts, Texas, and California.[4]

26. Plaintiff received a Notice of the Data Breach on or around April 17, 2025. According to the notice Plaintiff received, her PII, including her Social Security number and name, were compromised in the Data Breach.

27. On information and belief, Defendant collects and maintains the highly private PII/PHI of employees, clients, and clients' employees, including information protected by HIPAA, unencrypted in its computer systems. Given the fact it is been in business since 1976, it has accumulated almost 50 years of client data.

28. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law. It did not.

---

[4] *Data Breach Notification, Kelly & Associates Insurance Group, Inc.,* MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/047b774f-2e79-4a04-9f4c-4dd7a8b2ee8d.html (last visited April 21, 2025); *Security Breach Notifications,* NEW HAMPSHIRE ATTORNEY GENERAL, https://www.doj.nh.gov/citizens/consumer-protection-antitrust-bureau/security-breach-notifications (last visited April 21, 2025); *Security Breach Notices,* SC DEPARTMENT OF CONSUMER AFFAIRS, https://consumer.sc.gov/identity-theft-unit/security-breach-notices (last visited April 21, 2025); *Data Breach Notification Reports,* MASS.GOV, https://www.mass.gov/lists/data-breach-notification-reports (last visited April 21, 2025); *Data Security Breach Reports,* KEN PAXTON ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited April 21, 2025); *Search Data Security Breaches,* ROB BONTA ATTORNEY GENERAL OF CALIFORNIA, https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=https%3A%2F%2Foag.my.site.com%2Fdatasecuritybreachreport%2Fapex%2FDataSecurityReportsPage&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last visited April 21, 2025).

29. Between December 12, 2024, to December 17, 2024, cybercriminals had unfettered access to Defendant's network and accessed extremely sensitive PII, including social security numbers.

30. As evidenced by the Data Breach, Defendant's cybersecurity systems were completely inadequate and allowed cybercriminals to steal files containing a treasure trove of highly private information belonging to its employees, clients, and clients' employees.

31. Defendant waited until April 9, 2025, or at least 118 days, before it started notifying victims of the Data Breach.

32. 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.

33. Moreover, given Defendant's inadequate and vague Breach Notice, Plaintiff is left wondering what information was actually accessed.

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

35. In response to the Data Breach, Defendant does not contend that it has made any changes to or implemented any additional security measures, but rather, that it "will continue to review its already robust security policies." Ex. 1. The fact Defendant did not even discovery the Data Breach for at least five days (December 12, 2024 to December 17, 2024) suggests that Defendant's security policies are far from robust, and adequate security measures should have been in place before the Data Breach.

36. Through its Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, providing monitoring services, and advising Plaintiff "to

remain vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports." *Id.*

37. Despite recognizing the harm that flowed from the Data Breach, 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/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

38. On information and belief, Defendant has offered identity monitoring services to some victims, for twelve months, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the information compromised involves PII/PHI that cannot be changed, such as Social Security numbers. *Id.*

39. 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.

40. 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 here, Social Security numbers were 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.

41. 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 them to lose control over the PII of its employees, clients, and clients' employees. Defendant's negligence is evidenced by its failure to prevent the Data Breach, and its

continued inability to determine the exact information that was accessed, despite the significant amount of time that has passed between December 12, 2024, and present.

42. Furthermore, Defendant obfuscates the nature of the Data Breach and the threat it posed. The Notice fails to disclose who exactly was impacted (employees, clients, employees of clients, etc.), how many people were impacted, how the Data Breach happened including how cybercriminals were able to avoid detection for no less than *five days*, exactly what information was compromised, or why it took the Defendant four months months before it finally began notifying some victims that cybercriminals had gained access to their highly private information.

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

43. It is well known that PII is an invaluable commodity and a frequent target of hackers. Defendant's data security obligations were particularly important given the nature of its business, and the substantial increase in cyberattacks and/or data breaches in recent years.

44. Employee benefit plans face significant cybersecurity threats and, given the incredibly significant amount of assets involved, the consequences of even one single attack can be devastating.

45. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[5]

46. 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

[5] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter. org/publication/2024-data-breach-report/ (last visited April 13, 2025).

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."[6]

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

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

49. 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.

50. 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 Experiences and Injuries

51. Defendant obtained Plaintiff's PII/PHI from her current employer, who employs Defendant's services for benefits administration. And as a result, Plaintiff was injured by the Data Breach.

---

[6] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (published Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited April 13, 2025).

52. Plaintiff (or her third-party agent) provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

53. Plaintiff (or her third-party agent) reasonably understood that a portion of the funds paid to Defendant for services would be used to pay for adequate cybersecurity and protection of PII/PHI.

54. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff's PII, including at least her name and Social Security number. And upon information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

55. To the best of her knowledge, Plaintiff's PII has not been compromised in any prior data breaches.

56. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

57. Because of the Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

58. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

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

60. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

61. Indeed, following the Data Breach, Plaintiff began experiencing a lot of spam and scam text messages and phone calls, including messages about insurance (which Defendant provide to businesses), suggesting that her PII has been placed in the hands of cybercriminals.

62. On information and belief, Plaintiff's phone number was also compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, to gather and steal even more information.

63. Because of the Data Breach, Plaintiff spent time placing a lock on her credit, and anticipates spending additional considerable amounts of time and money trying to mitigate her injuries.

64. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

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

66. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses,

lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

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

68. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen

private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

69. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

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

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

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

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

members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

74. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, extortion, and exposure of stolen PII.

75. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them 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.

Consumers Prioritize Data Security

76. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[7] Therein, Cisco reported the following:

i. "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."[8]

[7] *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 April 14, 2025).
[8] *Id*. at 3.

j. "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."[9]

k. 89% of consumers stated that "I care about data privacy."[10]

l. 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.[11]

m. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[12]

n. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[13]

Defendant Failed to Follow FTC Guidelines

86. 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.

87. 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;

[9] *Id.*
[10] *Id.* at 9.
[11] *Id.*
[12] *Id.*
[13] *Id.* at 11.

d. understand its network's vulnerabilities; and

e. implement policies to correct security problems.

88. 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.

89. 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.

90. 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.

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

Defendant Failed to Follow Industry Standards

92. 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.

93. 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.

94. 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.

95. 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.

Defendant Violated HIPAA

96. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[14]

97. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

- failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

[14] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

- failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

98. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

99. 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/PHI was compromised in the Data Breach of Defendant's network, including all those individuals who received notice of the breach.

100. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors,

any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

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

102. 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.

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

104. **Numerosity.** The Class members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes thousands of members.

105. **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 were negligent in maintaining, protecting, and securing PII;

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

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

f. if Defendant's Breach Notice was reasonable;

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

h. what the proper damages measure is; and

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

106. **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.

107. **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.

108. **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.

109. **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)

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

111. Plaintiff and the Class 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.

112. 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.

113. 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.

114. 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.

115. 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.

116. 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.

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

118. 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.

119. 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 (or their third party agents) entrusted Defendant with their confidential PII, a necessary part of obtaining employment and Defendant's services.

120. 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.

121. 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.

122. 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.

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

124. 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.

125. 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.

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

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

128. 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.

129. 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)

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

131. 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.

132. 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.

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

134. 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's 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.

135. 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.

136. Defendant's violations of the California Consumer Records Act, Cal. Civ. Code § 1798.80, *et seq.,* and the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, provide an independent basis for Plaintiff's negligence *per se* claim.

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

138. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its 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.

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

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

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

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

142. Defendant offered to provide services to Plaintiff and members of the Class (or their third-party agents) if, and in exchange, Plaintiff and members of the Class provided Defendant with their PII.

143. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized persons.

144. Plaintiff and the members of the Class (or their third-party agents) accepted Defendant's offer by providing PII to Defendant in exchange for Defendant's services.

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

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

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

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

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

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

148. 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).

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

150. 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.

151. 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.

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

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

154. 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.

155. 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.

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

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

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

158. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their Private Information to facilitate its business, and (2) from accepting their payment.

159. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

160. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

161. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information.

162. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security

obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

163. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their Private Information.

164. Plaintiff and Class members have no adequate remedy at law.

165. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

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

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

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

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

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

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

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

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

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

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

174. 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.

175. Specifically, Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations and Privacy Policy. Defendant's disclosure of Plaintiff's PII is highly offensive to the reasonable person.

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

177. 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 constitute an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

178. 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.

179. 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.

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

181. 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.

182. 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.

183. 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.

184. 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.

185. 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.

186. 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
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

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

188. 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.

189. 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.

190. 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 breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

191. 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.

192. 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.

193. 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.

194. 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.

195. 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

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: April 22, 2025

By: */s/ Duane O. King*

Duane O. King Bar No: 19430
THE LAW OFFICES OF DUANE O. KING, PC
803 W. Broad St., Suite 210
Falls Church, VA 22046
Telephone: (202) 331-1963
dking@dkinglaw.com

Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

**pro hac vice* forthcoming

Attorneys for Plaintiff and the Proposed Class