Exhibit A

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

IN RE: KNIGHT BARRY TITLE, INC. DATA INCIDENT LITIGATION This Document Relates To: All Actions	Case No. 2:24-cv-00211-LA **JURY TRIAL DEMANDED**

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Brenda Raner, Julie Lewandowski, Toby Johnson, and Michael Mullarkey (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Defendant Knight Barry Title, Inc. ("KBT" or "Defendant"). Plaintiffs bring this action by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by their counsel as to all other matters, as follows.

I. INTRODUCTION

1. Knight Barry Title, Inc. is a title insurance company headquartered in Racine, Wisconsin. It operates 80 locations throughout Wisconsin, Minnesota, Michigan, Florida, and Texas.

2. As part of its operations, KBT collects, maintains, and stores highly sensitive personal information belonging to its clients, including, but not limited to their "personally identifying information" (*i.e.*, "PII") such as full names, addresses, and Social Security numbers, and government-issued IDs, as well as financial account information (collectively, "Private Information").

3. On July 25, 2023, KBT experienced a data breach incident in which unauthorized cybercriminals accessed its information systems and databases and stole Private Information belonging to Plaintiffs and Class members (the "Data Breach"). KBT discovered this unauthorized

access on August 15, 2023. Subsequent investigation by KBT determined that the unauthorized actors were able to access and steal Private Information concerning Plaintiffs and Class members.

4. On February 1, 2024, KBT sent a notice to individuals whose information was accessed in the Data Breach.

5. Because KBT stored and handled Plaintiffs' and Class members' highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Ultimately, KBT failed to fulfill this obligation, as unauthorized cybercriminals breached KBT's information systems and databases and stole vast quantities of Private Information belonging to KBT's clients, including Plaintiffs and Class members. This Data Breach—and the successful exfiltration of Private Information—were the direct, proximate, and foreseeable results of multiple failings on the part of KBT.

7. The Data Breach occurred because KBT failed to implement reasonable security protections to safeguard its information systems and databases. Thereafter, KBT failed to timely detect this Data Breach until 21 days after the Data Breach occurred. Moreover, before the Data Breach occurred, KBT failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been made aware of this fact, they would have never provided such information to KBT.

8. KBT's subsequent handling of the breach was also deficient. KBT delayed notifying victims of the Breach until February 1, 2024—170 days (***nearly 6 months***) after KBT discovered the Data Breach.

9. Further, KBT's meager attempt to ameliorate the effects of the Data Breach with 1 year of complimentary credit monitoring is inadequate. Much of the Private Information that was

stolen is immutable and 1 year of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

10. As a result of KBT's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs and Class members suffered injuries, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

11. Accordingly, Plaintiffs brings this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification to Plaintiffs and Class members that their Private Information had been compromised; and for Defendant's failure to inform Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Brenda Rander

12. Plaintiff Brenda Rander is a resident and citizen of Milwaukee, Wisconsin. Plaintiff Rander was a client of KBT. Plaintiff Raner received Defendant's Data Breach Notice.

Plaintiff Julie Lewandowski

13. Plaintiff Julie Lewandowski is a resident and citizen of Germantown, Wisconsin. Plaintiff Lewandowski is a former client of KBT. Plaintiff Lewandowski received Defendant's Data Breach Notice.

Plaintiff Toby Johnson

14. Plaintiff Toby Johnson is a resident and citizen of Kaukauna, Wisconsin. Plaintiff Johnson obtained services at Defendant in approximately 2020. Plaintiff Johnson received Defendant's Data Breach Notice.

Plaintiff Michael Mullarkey

15. Plaintiff Michael Mullarkey is a resident and citizen of Lake Forest, Illinois. Plaintiff Mullarkey is a former client of KBT. Plaintiff Mullarkey received Defendant's Data Breach Notice.

Defendant Knight Barry Title, Inc.

16. The Knight Barry Title, Inc. is a Wisconsin corporation with its principal place of business located at 400 Wisconsin Ave., Racine, WI 53403. Defendant is headquartered in this District and operates in Wisconsin, Minnesota, Michigan, Florida, and Texas.

III. JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at

least one Class member (including Plaintiff Mullarkey) is a citizen of a state different from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Racine, Wisconsin.

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 Plaintiffs' and Class members' claims occurred in this District and because Defendant resides in this District.

IV. FACTUAL ALLEGATIONS

A. Knight Barry Title, Inc. – Background

20. Knight Barry Title is a title insurance company founded in 1918 that operates in Wisconsin, Minnesota, Michigan, Florida, and Texas. As part of its normal operations, KBT collects, maintains, and stores large volumes of Private Information belonging to its current and former clients.

21. Plaintiffs and Class members are current and former customers of Defendant.

22. In the course of their relationship, and as a condition of obtaining Defendant's services, Plaintiffs and Class members were required to provide Defendant with their Private Information.

23. Plaintiffs and Class members made their Private Information available to KBT with the reasonable expectation that KBT would provide confidentiality and adequate security to keep the sensitive and private information secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, Defendant would provide them with prompt and accurate notice.

24. This expectation was objectively reasonable and based on KBT's representations, and obligations imposed by statute, regulations, industrial customs, and standards of general due care.

25. KBT represents on its website that:

> We will use our best efforts to ensure that no unauthorized parties have access to any of your information. We restrict access to NPI[1] about you to those employees that need to know that information to provide products or services to you. We will use our best efforts to train and oversee our employees and agents to ensure that your information will be handled responsibly and in accordance with this Privacy Policy. We currently maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your NPI. [2]

26. KBT failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of KBT's current and former clients—Plaintiffs and Class members.

27. Unfortunately for Plaintiffs and Class members, KBT failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

28. According to Defendants' public statements, cybercriminals breached KBT's information systems on or about July 25, 2023.

---

[1] "Non-public personal information ('NPI') is nonpublic information about you that we obtain in connection with providing a financial product or service to you, such as title products or closing and settlement services. NPI does not include publicly available information, such as information in government records or real estate records; that information is not protected from disclosure because of its public nature." *Knight Barry Title Group Privacy Policy*, available at https://www.knightbarry.com/privacy#:~:text=We%20request%20information%20from%20you,2)%20as%20permitted%20by%20law (last accessed February 6, 2024).

[2] *Id*.

29. KBT did not discover this intrusion until twenty-one days later, on August 15, 2023. It took a further two days for KBT to secure its systems. KBT publicly described the Data Breach as follows:

> On August 15, 2023, Knight Barry discovered suspicious activity on our computer network and that certain files were encrypted with malware. Upon discovery of this activity, Knight Barry took immediate steps to ensure the security of the network and restore the systems. Systems were restored and brought back online by August 17, 2023. Knight Barry also launched an investigation into the nature and scope of the event. The investigation determined that between July 25, 2023 and August 15, 2023, an unauthorized actor gained access to Knight Barry systems and may have accessed or acquired data on certain systems.

30. KBT sent notice of the Data Breach to affected individuals on February 1, 2024—191 days after the Breach and 170 days after KBT discovered the breach.

31. Omitted from KBT's public statements concerning the Data Breach is any information concerning the root cause of the Data Breach, the vulnerability exploited, and the remedial measures taken to ensure that a breach does not happen again.

C. KBT's Many Failures Both Prior to and Following the Breach

32. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiffs and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

33. First, Defendant inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

34. Second, Defendant failed to timely detect the Data Breach, only becoming aware of the intrusion twenty-one days after the Breach, during which time cybercriminals freely accessed and stole the sensitive Private Information belonging to Defendant's clients.

35. Third, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendant did not

have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendant.

36. In addition to the failures that lead to the successful breach, Defendant's failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiffs and Class members.

37. Defendant's more than 6-month delay in informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

38. Additionally, Defendant's attempt to ameliorate the effects of the Data Breach with limited complimentary credit monitoring is inadequate. Plaintiffs' and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. This can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. The harm is more acute as much of the stolen Private Information, such as Social Security numbers, is immutable.

39. In short, Defendant's myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiffs and Class members that their Private Information had been stolen, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information for 191 days before Defendant finally granted victims the

opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

40. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

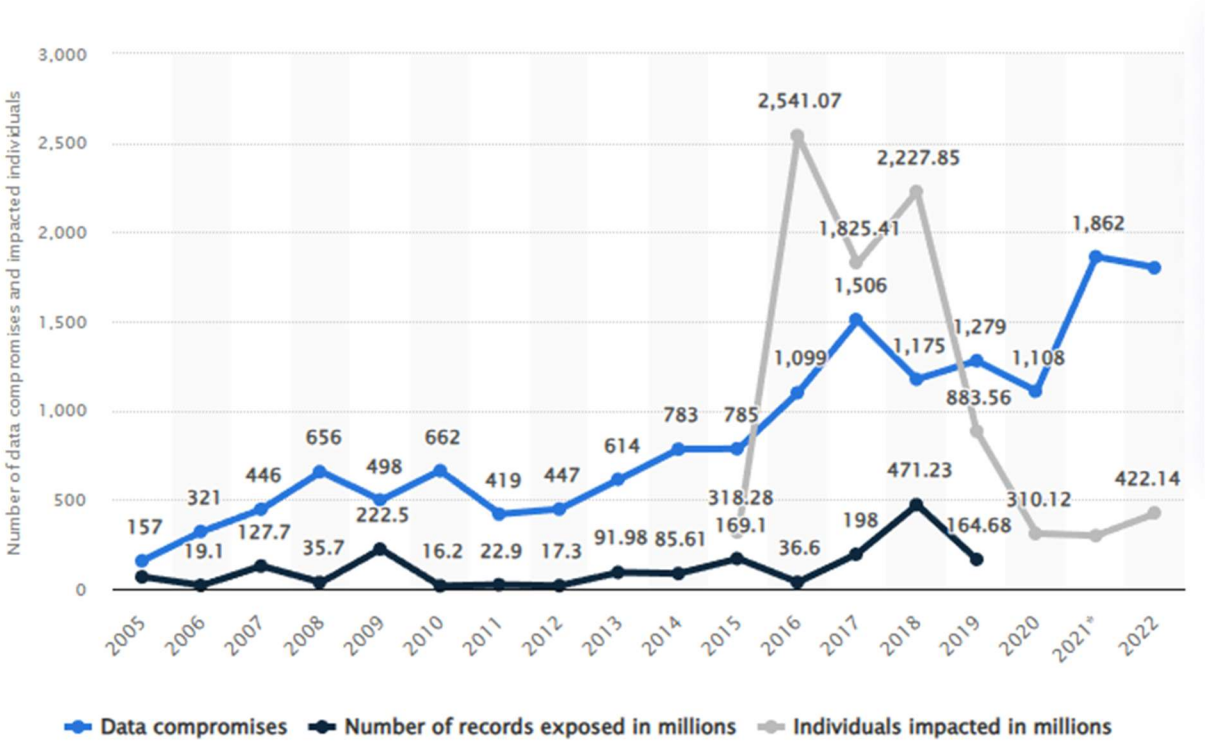
41. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[3]

42. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[4] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[5]

[3] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.

[4] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[5] *Id.*



43. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with social security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[6]

44. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

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

[6] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

45. This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[8]

46. Given the nature of Defendant's Data Breach, as well as the length of the time Defendant's networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in their names.

47. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[9] The

---

[7] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[8] *Id.*

[9] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at

information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

48. To date, Defendant has offered its consumers only limited identity theft monitoring services. The services offered are inadequate to protect Plaintiffs and Class members from the threats they will face for years to come, particularly in light of the Private Information at issue here.

49. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from misappropriation. As a result, the injuries to Plaintiffs and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former clients.

E. Defendant Had a Duty and Obligation to Protect Private Information

50. Defendant has an obligation to protect the Private Information belonging to Plaintiffs and Class members. First, this obligation was mandated by government regulations and state laws, including FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII. Third, Defendant imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiffs and Class members provided,

---

https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. FTC Act Requirements and Violations

51. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

52. 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.[10] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[11] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a

[10] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed August 15, 2023).
[11] *Id.*

breach.[12] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

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

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

56. Similarly, the Wisconsin data breach notification law, Wis. Stat. 134.98, obligates entities whose principal place of business is located in Wisconsin, or who maintain personal information concerning residents of Wisconsin, to provide notice to victims of unauthorized acquisition of personal information within 45 days of discovery of a data breach. Wis. Stat. 134.94(3).

[12] *Id.*

57. Defendant was fully aware of its obligation to protect the Private Information of its current and former clients, including Plaintiffs and Class members. Defendant is a sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its clients' PII.

58. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

2. Industry Standards and Noncompliance

59. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

60. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

61. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as

firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

62. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

3. Defendant's Own Stated Policies and Promises

64. Defendant's own published privacy policy states the following:

> We will use our best efforts to ensure that no unauthorized parties have access to any of your information. We restrict access to NPI[13] about you to those employees that need to know that information to provide products or services to you. We will use our best efforts to train and oversee our employees and agents to ensure that your information will be handled responsibly and in accordance with this Privacy Policy. We currently maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your NPI.[14]

---

[13] "Non-public personal information ('NPI') is nonpublic information about you that we obtain in connection with providing a financial product or service to you, such as title products or closing and settlement services. NPI does not include publicly available information, such as information in government records or real estate records; that information is not protected from disclosure because of its public nature." *Knight Barry Title Group Privacy Policy*, available at https://www.knightbarry.com/privacy#:~:text=We%20request%20information%20from%20you,2)%20as%20permitted%20by%20law (last accessed February 6, 2024).

[14] *Id.*

65. Defendant failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information belonging to Plaintiffs and Class members.

F. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

66. Like any data hack, the Data Breach presents major problems for all affected.[15]

67. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

68. The ramifications of Defendant's failure to properly secure Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

69. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

70. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

---

[15] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

[16] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

71. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[17] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[18]

72. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

73. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[19]

74. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with just one year of credit monitoring. However, this is inadequate to protect victims of the Data Breach from the lifelong risk of harm imposed on them by Defendant's failures.

---

[17] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.

[18] *Id.*

[19] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.

75. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

76. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, the imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

77. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within the limited time of credit monitoring offered by Defendant.

78. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

79. Plaintiffs retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFFS

i. Plaintiff Brenda Raner

80. Plaintiff Raner is a former client of KBT. As a condition of receiving services from KBT, Plaintiff Raner was required to provide KBT her Private Information.

81. Plaintiff Raner is very careful about sharing her Private Information. Plaintiff Raner stores documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured means. Plaintiff Raner would not have trusted her Private Information to Defendant had she known of Defendant's deficient data security practices.

82. Plaintiff Raner received KBT's Data Breach notice. The notice informed Plaintiff Rander that her Private Information was improperly accessed and obtained by third parties.

83. After the Data Breach, Plaintiff Raner experienced a notable increase in the amount of spam calls and emails received.

84. As a result of the Data Breach, Plaintiff Raner has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Raner has also spent several hours dealing with the Data

Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

85. As a result of the Data Breach, Plaintiff Raner has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Raner is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

86. Plaintiff Raner suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

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

ii. Plaintiff Julie Lewandowski

88. Plaintiff Julie Lewandowski is a previous client of KBT. As a condition of receiving services from KBT, Plaintiff Lewandowski was required to provide KBT her Private Information.

89. Plaintiff Lewandowski is very careful about sharing her Private Information. Plaintiff Lewandowski stores documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the

internet or any other unsecured means. Plaintiff Lewandowski would not have trusted her Private Information to Defendant had she known of Defendant's deficient data security practices.

90. Plaintiff Lewandowski received KBT's Data Breach notice. The notice informed Plaintiff Lewandowski that her Private Information was improperly accessed and obtained by third parties.

91. After the Data Breach, Plaintiff Lewandowski experienced a notable increase in the amount of spam calls and emails received.

92. As a result of the Data Breach, Plaintiff Lewandowski has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Lewandowski has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

93. As a result of the Data Breach, Plaintiff Lewandowski has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Lewandowski is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

94. Plaintiff Lewandowski suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained

from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

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

iii. Plaintiff Toby Johnson

96. Plaintiff Toby Johnson is a previous client of KBT. As a condition of receiving services from KBT, Plaintiff Johnson was required to provide KBT his Private Information.

97. Plaintiff Johnson is very careful about sharing his Private Information. Plaintiff Johnson stores documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured means. Plaintiff Johnson would not have trusted his Private Information to Defendant had he known of Defendant's deficient data security practices.

98. Plaintiff Johnson received KBT's Data Breach notice. The notice informed Plaintiff Johnson that his Private Information was improperly accessed and obtained by third parties.

99. After the Data Breach, Plaintiff Johnson experienced a notable increase in the amount of spam calls and emails received.

100. As a result of the Data Breach, Plaintiff Johnson has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Johnson has also spent several hours dealing with the

Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

101. As a result of the Data Breach, Plaintiff Johnson has suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his Private Information for purposes of identity theft and fraud. Plaintiff Johnson is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

102. Plaintiff Johnson suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

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

iv. Plaintiff Michael Mullarkey

104. Plaintiff Michael Mullarkey is a previous client of KBT. As a condition of receiving services from KBT, Plaintiff Mullarkey was required to provide KBT his Private Information.

105. Plaintiff Mullarkey is very careful about sharing his Private Information. Plaintiff Mullarkey stores documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or

any other unsecured means. Plaintiff Mullarkey would not have trusted his Private Information to Defendant had he known of Defendant's deficient data security practices.

106. Plaintiff Mullarkey received KBT's Data Breach notice. The notice informed Plaintiff Mullarkey that his Private Information was improperly accessed and obtained by third parties.

107. As a result of the Data Breach, Plaintiff Mullarkey has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Mullarkey has also spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

108. As a result of the Data Breach, Plaintiff Mullarkey has suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his Private Information for purposes of identity theft and fraud. Plaintiff Mullarkey is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

109. Plaintiff Mullarkey suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

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

V. CLASS REPRESENTATION ALLEGATIONS

111. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

112. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process. According to a report submitted to the Office of the Maine Attorney General, the Data Breach affected at least 44,910 individuals.[20] The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

113. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over

[20] https://apps.web.maine.gov/online/aeviewer/ME/40/2a17e4a8-27cb-41a4-b17b-6a8822e5e4d1.shtml

the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

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

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

f. Whether Defendant owed a duty to safeguard their Private Information;

g. Whether Defendant breached its duty to safeguard Private Information;

h. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

i. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

j. Whether Defendant's conduct violated the FTCA;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant was unjustly enriched;

n. What damages Plaintiffs and Class members suffered as a result of Defendant's misconduct;

o. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiffs and Class members are entitled to additional credit or identity monitoring and monetary relief.

114. Typicality: Plaintiffs' claims are typical of the claims of the Class as Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

115. Adequacy: Plaintiffs are adequate class representatives because Plaintiffs' interests do not materially or irreconcilably conflict with the interests of the Class Plaintiffs seek to represent, Plaintiffs have retained counsel competent and highly experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor Plaintiffs' counsel have any interests that are antagonistic to the interests of other members of the Class.

116. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiffs on behalf of the Class)

117. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

118. Defendant owes a duty of care to protect the Private Information belonging to Plaintiffs and Class members. Defendant also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect clients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiffs and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

119. Defendant owes this duty because it had a special relationship with Plaintiffs' and Class members. Plaintiffs and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

120. Defendant also owes this duty because industry standards mandate that Defendant protect its clients' confidential Private Information.

121. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiffs and Class members. This duty exists to provide Plaintiffs and Class members with the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

122. Defendant breached its duties owed to Plaintiffs and Class members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their Private Information.

123. Defendant also breached the duties it owed to Plaintiffs and Class members by failing to timely and accurately disclose to them that their Private Information had been improperly acquired and/or accessed.

124. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanent increased risk of identity theft.

125. Plaintiffs and Class members were foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

126. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiffs and Class members.

127. Plaintiffs and the Class are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiffs on behalf of the Class)

128. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

129. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a duty on Defendant to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiffs and Class members.

130. The Wisconsin data breach notification law, Wis. Stat. 134.98, obligates entities whose principal place of business is located in Wisconsin, or who maintain personal information concerning residents of Wisconsin, to provide notice to victims of unauthorized acquisition of personal information within 45 days of discovery of a data breach. Wis. Stat. 134.94(3).

131. Defendant breached these duties by:

a. failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class members' Private Information;

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

c. allowing unauthorized access to Plaintiffs' and Class members' Private Information;

d. failing to detect in a timely manner that Plaintiffs' and Class members' Private Information had been compromised;

e. failing to remove former customers' Private Information that it was no longer required to retain pursuant to regulations; and

f. filing to timely and adequately notify Plaintiffs and Class members about the existence and scope of the Data Breach, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

132. Defendant's failure to comply with these duties constitutes negligence *per se*.

133. Plaintiffs and Class members are within the class of persons that the FTCA and Wisconsin data breach notification statute were intended to protect.

134. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class members' Private Information in compliance with applicable laws and industry standards would result in that Private Information being accessed and stolen by unauthorized actors.

135. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

136. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiffs on behalf of the Class)

137. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

138. Plaintiffs and Class members provided Defendant with their Private Information.

139. By providing their Private Information, and upon Defendant's acceptance of this information, Plaintiffs and the Class, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

140. The implied contracts between Defendant and Plaintiffs and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

141. The implied contracts for data security also obligated Defendant to provide Plaintiffs and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

142. Defendant breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiffs and Class members; allowing unauthorized persons to access Plaintiffs' and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class members, as alleged above.

143. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiffs on behalf of the Class)

144. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

145. This count is brought in the alternative to Count III.

146. Plaintiffs and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

147. Defendant was benefitted by the conferral of Plaintiffs' and Class members' Private Information and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

148. Defendant also understood and appreciated that Plaintiffs' and Class members' Private Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

149. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided or authorized their Private Information to be provided to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining clients, gaining the reputational advantages conferred upon it by Plaintiffs and Class members, collecting excessive advertising and sales revenues as described

herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

150. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

151. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

152. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class members in an unfair and unconscionable manner.

153. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

154. Defendant is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the

value to Defendant of the PII that was accessed and exfiltrated in the Data Breach and the profits Defendant receives from the use and sale of that information.

155. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

156. Plaintiffs and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
INVASION OF PRIVACY
(By Plaintiffs on behalf of the Class)

157. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

158. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information that Defendant possessed and/or continues to possess.

159. By failing to keep Plaintiffs' and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

160. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Defendant's actions highly offensive.

161. Defendant invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

162. As a proximate result of such misuse and disclosures, Plaintiffs' and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

163. In failing to protect Plaintiffs' and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiffs' and Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of clients. Plaintiffs, therefore, seeks an award of damages, including punitive damages, individually and on behalf of the Class.

COUNT VI
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(By Plaintiffs on behalf of the Class)

164. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

165. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

166. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

167. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and financial information and storage of other personal

information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

168. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court award Plaintiffs and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

F. That the Court award pre- and post-judgment interest at the maximum legal rate;

G. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

H. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of the putative Class, demand a trial by jury on all issues so triable.

Date: October 7, 2024 Respectfully Submitted,

/s/ Nickolas J. Hagman
Nickolas J. Hagman
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
nhagman@caffertyclobes.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

Kevin Laukaitis
LAUKAITIS LAW LLC
954 Avenida Ponce De León
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Interim Co-Lead Class Counsel

Anthony Procaccio
A. PROCACCIO LAW OFFICE, S.C.
1433 N. Water St., Suite 400
Milwaukee, WI 53202
T: (414) 644-0321
anthony@aprolawoffice.com

Plaintiffs' Interim Liaison Counsel

CERTIFICATE OF SERVICE

I, Nickolas J. Hagman, an attorney, hereby certify that on October 7, 2024, service of the foregoing ***Amended Consolidated Class Action Complaint*** was accomplished through the Court's electronic filing system.

/s/ Nickolas J. Hagman
Nickolas J. Hagman