IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In re Turner Construction Company Data Breach Litigation.	Lead Case No. 1:26-cv-07103 Judge: Hon. Denise Cote **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMAND**

Plaintiffs David Reed, Jaden Dias, George R. Booth, Johnny Hewett, Joshua Donald, Louis Martinelli, Cayden Anthony, Bill Bishop, and Mustafa Arsiwala ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members," as defined below), by and through their undersigned counsel, file this Class Action Complaint against Turner Construction Company ("Turner" or "Defendant") and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of their counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit against Defendant for its negligent failure to protect and safeguard Plaintiffs' and Class Members' highly sensitive personally identifiable information[1] ("PII" or "Private Information"), culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of Defendant's failure to implement

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

reasonable and necessary data security practices, cybercriminals easily infiltrated Defendant's inadequately protected computer systems and ***stole*** the Private Information of Plaintiffs and Class Members.

2. Defendant is major U.S. construction and general contracting company that provides construction management, general contracting, and related services for commercial, healthcare, education, infrastructure, and other large-scale projects.[2]

3. In the ordinary course of its business, and as a condition of employment, Defendant collects, stores, and maintains employees' PII, including Plaintiffs' and Class Members' PII. Plaintiffs and Class Members are current and former employees of Defendant.

4. Between approximately July 2, 2026, and July 15, 2026, unauthorized cybercriminals gained access to Defendant's inadequately protected computer system and extracted Plaintiffs' and the Class Member's Private Information stored thereon.[3] Upon information and belief, Defendant has not publicly disclosed the threat actor responsible for the Data Breach. Alarmingly, however, on August 12, 2026, the ransomware group, PayoutsKING ("Payouts King") claimed responsibility for the Data Breach and theft of Plaintiffs' and Class Members' PII.[4]

5. The Defendant disclosed in its notice letter ("Notice Letter") to affected individuals that at least the following pieces of sensitive personal information were included in the Breach:

[2] https://www.turnerconstruction.com/services (last visited Oct. 7, 2026); *see also* https://www.turnerconstruction.com/projects (last visited Oct. 7, 2026); https://www.turnerconstruction.com/who-we-are (last visited Oct. 7, 2026).
[3] https://mm.nh.gov/files/uploads/doj/remote-docs/turner-construction-20260818.pdf (last visited Oct. 7, 2026).
[4] https://www.breachsense.com/breaches/turner-construction-data-breach/ (last visited Oct. 14, 2026).

names, Social Security numbers, dates of birth, salary, bank account information used for direct deposits, home addresses, and, for a limited number of people, passport numbers.[5]

6. While the Breach started on or about July 2, 2026, Turner delayed noticing affected individuals until around August 18, 2026, when Turner began mailing Notice Letters to affected individuals.[6] Defendant's delay in alerting impacted individuals of the Breach prevented Plaintiffs and Class Members from taking earlier actions to protect themselves against fraud and misuse of their information.

7. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard their Private Information from unauthorized disclosure and would implement sufficient cybersecurity safeguards to protect such information.

8. Businesses that store and maintain employees' Private Information, like Defendant, owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from unauthorized disclosures and unauthorized third parties. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons, and especially hackers, will harm the affected individuals, including to the invasion of their private information and financial matters.

9. In providing their Private Information to Defendant, Plaintiffs and the Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and secured from unauthorized disclosures, to use this information for business

[5] Exhibit 1
[6] *Id.*

purposes only, and to disclose it only as authorized. Defendant failed to do so, resulting in the unauthorized disclosure of Plaintiffs' and Class Members' Private Information in the Breach.

10. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect individuals' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

11. Upon information and belief, Plaintiffs' and Class Members' Private Information is in the hands of cybercriminals who will continue to use the stolen Private Information for nefarious purposes for the rest of their lives.

12. Due to Defendant's negligent failure to secure and protect Plaintiffs' and Class Members' Private Information, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

13. As a result of the Data Breach, upon information and belief, Plaintiffs' Private Information is available on the dark, or will soon be posted on the dark web, as that is the *modus operandi* of cybercriminals who target companies, like Defendant, to steal sensitive personal information for personal gain.

14. Now, and for the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft will have to spend time responding

to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

15. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

16. Defendant disregarded the rights of Plaintiffs and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiffs' and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

17. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft and misuse of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and

available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

18. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

II. THE PARTIES

Plaintiffs

19. Plaintiff **David Reed** is an individual, and at all relevant times, domiciled in and citizen of Thronton, Colorado. Plaintiff Reed received a Notice Letter from the Defendant informing him that his sensitive personal information was involved in the Breach.

20. Plaintiff **Jaden Dias** is an individual, and all relevant times, was domiciled in and a citizen of Milwaukee, Wisconsin. Plaintiff Dias received a Notice Letter from Defendant informing him that his sensitive personal information was involved in the Breach.

21. Plaintiff **George R. Booth** is an individual, and at all relevant times, domiciled in and citizen of Bellrose, New York. Plaintiff Booth received a Notice Letter from the Defendant informing him that his sensitive personal information was involved in the Breach.

22. Plaintiff **Johnny Hewett** is an individual, and at all relevant times, domiciled in and citizen of Ocean Springs, Mississippi. Plaintiff Hewett received a Notice Letter from the Defendant informing him that his sensitive personal information was involved in the Breach.

23. Plaintiff **Joshua Donald** is an individual, and at all relevant times, domiciled in and citizen of Brockton, Massachusetts. Plaintiff Donald received a Notice Letter from the Defendant informing him that his sensitive personal information was involved in the Breach.

24. Plaintiff **Louis Martinelli** is an individual, and at all relevant times, domiciled in and citizen of Forrest Hills, New York. Plaintiff Martinelli received a Notice Letter from the Defendant informing her that her sensitive personal information was involved in the Breach

25. Plaintiff **Bill Bishop** is an individual, and at all relevant times, domiciled in and a citizen of Colonial Beach, Virginia. Plaintiff Bishop received a Notice Letter from Defendant informing him that his sensitive personal information was involved in the Breach.

26. Plaintiff **Mustafa Arsiwala** is an individual, and at all relevant times, domiciled in and a citizen of Novi, Michigan. Plaintiff Arsiwala received a Notice Letter from Defendant informing him that his sensitive personal information was involved in the Breach.

Defendant

27. Defendant **Turner Construction Company** is a New York corporation with its headquarters and principal place of business located at 66 Hudson Boulevard East, New York, New York 10001.

III. JURISDICTION AND VENUE

28. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) numerous Class Members and at least one Plaintiff are citizens of a different state that is diverse from Defendant, and (4) there are more than 100 Class Members.

29. This Court has personal jurisdiction over Defendant because it is incorporated

under the laws of New York, its principal place of business is in New York, and the acts and omissions giving rise to Plaintiffs' claims occurred in this State.

30. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District, and a substantial part of the events, acts, and/or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and its Collection of Plaintiffs' and Class Members' Private Information.

31. Defendant is major U.S. construction and general contracting company that provides construction management, general contracting, and related services for commercial, healthcare, education, infrastructure, and other large-scale projects.[7]

32. As part of its business practices and to provide services, Defendant collects, stores, and maintains employees' PII, including Plaintiffs' and Class Members'. Plaintiffs and Class Members are current and former employees of Defendant.

33. Defendant obtains, collects, uses, and derives a benefit from the Private Information of Plaintiffs and Class Members. Defendant uses the Private Information it collects to provide employment and services, making a profit therefrom. Defendant would not be able to obtain revenue if not for the acceptance and use of Plaintiffs' and the Class's Private Information.

34. Defendant would be unable to engage in its regular business activities without collecting and aggregating Private Information it knows and understands to be sensitive and confidential.

[7] https://www.turnerconstruction.com/services (last visited Oct. 7, 2026); *see also* https://www.turnerconstruction.com/projects (last visited Oct. 7, 2026); https://www.turnerconstruction.com/who-we-are (last visited Oct. 7, 2026).

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

36. Class Members who are current and former employees of Defendant allowed Defendant to make a profit from their services and labor. Defendant promised data security to its employees as part of their employment and part of the revenue earned through the labor of its employees should have been specifically allocated to data security.

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

38. Defendant was aware of its duties to protect the Private Information from unauthorized disclosure, stating in tis Privacy Notice that:

> Turner takes the responsibility of keeping your information secure. The security measures Turner uses vary based on the sensitivity of the personal information we collect, process, and store, and the current state of technology. We also take measures to ensure service providers that process personal data on our behalf also have appropriate security measures.[8]

39. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

[8] https://www.turnerconstruction.com/privacy-notice (last visited Oct. 7, 2026).

40. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

42. Upon information and belief, Defendant failed to adopt reasonable and appropriate data security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiffs' and the Class's Private Information.

43. As a result of collecting and storing the Private Information of Plaintiffs and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs' and the Class Members' Private Information from disclosure to third parties, and to audit, monitor, and verify the integrity and cybersecurity of its systems storing Private Information.

B. Defendant's Data Breach.

44. Between approximately July 2, 2026, and July 15, 2026, unauthorized cybercriminals gained access to Defendant's inadequately protected computer system and extracted Plaintiffs' and the Class Member's Private Information stored thereon.[9] Upon information and belief, Defendant has not disclosed publicly what threat actor was involved.

[9] https://mm.nh.gov/files/uploads/doj/remote-docs/turner-construction-20260818.pdf (last visited Oct. 7, 2026).

45. The Defendant disclosed in its Notice Letter to affected individuals that at least the following pieces of sensitive personal information were included in the Breach: names, Social Security numbers, dates of birth, salary, bank account information used for direct deposits, home addresses, and, for a limited number of people, passport numbers.[10]

46. While the Breach started on or about July 2, 2026, Turner delayed noticing affected individuals until around August 18, 2026, when Turner began mailing Notice Letters to affected individuals.[11] Defendant's delay in alerting impacted individuals of the Breach prevented Plaintiffs and Class Members from taking earlier actions to protect themselves against fraud and misuse of their information.

47. Defendant acknowledges the imminent risk of fraud and identity theft Plaintiffs and Class Members now face by advising Plaintiffs and Class Members in the Notice Letter to "remain vigilant" by reviewing their bank, credit card, retirement, and other financial accounts for suspicious activity, enabling account alters and multi-factor authentication, reviewing their credit reports, considering credit freeze, be cautious of unexpected emails, texts messages, and telephone calls requesting personal of financial information, and contacting their financial institutions.[12]

48. Defendant's delayed notice of the Breach leaves impacted individuals with no information regarding critical facts about the Data Breach, such as details of the root cause of the Breach, the vulnerabilities exploited, whether Defendant was able to contain or end the cybersecurity threat, when Defendant first discovered the Data Breach, and the remedial measures taken by Defendant, if any. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity of information compromised in this specific

[10] Exhibit 1.
[11] *Id.*
[12] *Id.*

Breach.

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

50. Upon information and belief, the extortion group "Payout Kings" claimed responsibility for the Data Breach on its dark-web leak site, claiming to have exfiltrated roughly 27.2 terabytes of data from Turner. According to the ransomware group's post, the haul included engineering documents containing employees' personal data, military project files, legal and litigation records, correspondence, financial records, contracts and non-disclosure agreements.[13]

51. Payout Kings is a ransomware group that emerged in April 2025 and is notorious for stealing large amounts of data and selectively performs file encryption.[14] Payout Kings utilizes remote desktop protocol access, phishing templates, and cracked panel kits for initial access.[15] Payout Kings also adopts a victim-centric approach, quickly disclosing compromised data on leak sites.[16]

---

[13] Cyber Breaches, Turner Construction data breach (Payout Kings) (Aug. 18, 2026): https://www.cyberbreaches.org/en/incidents/turner-construction-2026-08-18 (last visited Oct. 8, 2026).
[14] https://www.zscaler.com/blogs/security-research/payouts-king-takes-aim-ransomware-throne (last visited Oct. 8, 2026).
[15] https://socradar.io/free-tools/ransomware-intelligence/groups/payoutsking (last visited Oct. 8, 2026).
[16] *Id.*

52. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

53. Upon information and belief, the Private Information was not encrypted prior to the Data Breach.

54. The cyberattack was targeted at Defendant as a company that collects and maintains valuable personal data from its many individuals, including Plaintiff and Class Members.

55. By collecting, storing, and maintaining the Private Information of Plaintiffs and Class Members, Defendant owed a duty to Plaintiffs and Class Members to protect and safeguard their Private Information from unauthorized disclosures.

56. Plaintiffs' and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Defendant's deficient security for employee data caused and allowed criminals to target and take files containing Plaintiffs' and Class Members' inadequately protected, unencrypted Private Information in Defendant's possession through the Data Breach.

57. Because Defendant had a duty to protect Plaintiffs' and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information. Thus, Defendant had a duty to ensure that employees' Private Information, stored within its networks and systems, was secured and protected from unauthorized disclosures to third parties.

58. Defendant could and should have prevented this Data Breach by ensuring the files and servers containing Plaintiffs' and Class Members' Private Information were properly secured and encrypted but failed to do so.

59. Defendant could have prevented the Data Breach by properly securing and encrypting the files and servers containing the Private Information of Plaintiffs and Class Members. This Data Breach could have been prevented through industry standard network segmentation and encryption of confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies

60. Plaintiffs further believe that their Private Information and that of Class Members, was subsequently sold or posted on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals, like Payout King, that commit cyber-attacks of this type.

61. By Payout King taking responsibility of the Data Breach and obtaining the Private Information of Plaintiffs and Class Members, the risk of fraud and identity theft is imminent and impending and not speculative. Now that Payout King have the necessary information of Plaintiffs and Class Members to commit fraud and identity theft, Plaintiffs and Class Members will remain at risk of fraud and identity theft for the rest of their lives.

62. Acknowledging the harm that the Data Breach presents, Defendant is offering victims limited complimentary credit monitoring services – an offer that is inadequate considering that victims of the Data Breach will likely suffer an increased risk of identity theft and other harms for years into the future now that their Private Information is in the hands of the ransomware group Payout King.

63. All in all, Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

64. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

65. As such, Plaintiffs and the Class have suffered harm and continue to be at an imminent and impending risk of identity theft and fraud, which is not speculative.

C. Cyber Criminals Will Use Plaintiffs' and Class Members' Private Information to Defraud them.

66. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

67. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[17]

68. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, obtain medical services, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[18]

69. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

---

[17] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 19, 2026).

[18] *See, e.g.*, Nikkita Walker, What Can You Do With Your Social Security Number, Credit.com (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

70. When cybercriminals manage to steal personally sensitive data like Social Security numbers—as they did here—there is no limit to the amount of fraud to which Plaintiffs and Class Members are exposed.

71. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[19]
>
> (Emphasis added).

72. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[20]

73. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking entities like Defendant is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

74. A Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[21]

---

[19] Dark Web Monitoring: What You Should Know, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[20] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737.
[21] Michael Kan, Here's How Much Your Identity Goes for on the Dark Web, PGMag (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

75. Identity theft experts advise victims of data breaches: "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[22]

76. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, **they will use it**.[23]

77. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

78. For instance, with a stolen Social Security number, which was information in possession by the Defendant and included in the Breach, criminals can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[25]

79. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[26]

---

[22] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[23] Ari Lazarus, *How fast will identity thieves use stolen info?*, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[24] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737 (emphasis added).
[25] *See* Nikkita Walker, *What Can Someone Do with Your Social Security Number?*, Credit.com (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[26] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

80. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

81. Defendant's offering of limited credit monitoring and theft protecting is wholly inadequate now that the ransomware group Payout King has claimed responsibility for the Data Breach. After the limited offering of credit monitoring and theft protection expires, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's negligence.

82. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft—it does not prevent identity theft.[27]

83. Nor can an identity monitoring service remove personal information from the dark web.[28]

84. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[29]

85. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and

[27] *See* Kayleigh Kulp, *Credit monitoring services may not be worth the cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.
[28] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[29] *Id.*

"alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come.

86. Even more serious is the identity restoration that Plaintiffs and other Class Members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

87. Plaintiffs and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property, including their Private Information;

c. Improper disclosure and theft of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;

f. Ascertainable losses in the form of time taken to respond to identity theft, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of diminution of the value of Plaintiffs' and Class Members' Private Information, for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

88. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches through the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

89. Plaintiffs and Class Members also have an interest in ensuring that their Private Information is removed from all Defendant's servers, systems, and files.

90. At the instruction of Defendant in the Notice Letter, Plaintiffs and Class Members are desperately trying to mitigate the damages Defendant caused them.

91. Given the kind of Private Information Defendant made accessible to hackers, however, Plaintiffs and the Class are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and

arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[30]

92. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware—or Should Have Been Aware—of the Risk of Cyberattacks.

93. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[31] Yahoo,[32] Marriott International,[33] Chipotle, Chili's, Arby's,[34] and others.[35]

94. The number of data breach victims has surpassed 1 billion for the first half of 2024, according to the Identity Theft Resource Center.[36]

95. Defendant should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII and PHI that it collected and maintained.

---

[30] *What happens if I change my Social Security number?*, Lexington Law (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[31] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[32] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[33] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Feb. 6, 2026).

[34] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[35] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[36] https://www.usatoday.com/story/money/2024/07/18/data-breach-what-to-do/74441060007/.

96. Defendant was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

97. Turner (1) had deficient security measures to protect the Private Information it stored for its current and former employees; (2) was aware or should have been aware of the risk of harm to its employees in the event of a data breach; (3) knew or should have known of the foreseeable harms caused by cyberattacks; and (4) negligently failed to safeguard Plaintiffs' and Class Members' Private Information.

98. As a result of Turner's deficient security measures to protect the Private Information of Plaintiffs and Class Members, the ransomware group Payout King now has possession of their Private Information and will use it for nefarious purposes. Thus, Plaintiffs' and Class Members are at imminent and impending risk of identity theft and fraud which is not speculative.

99. Despite its assurances to Plaintiffs and Class members regarding safeguarding Private Information, Defendant negligently failed to implement adequate security measures to safeguard the Private Information of Plaintiffs and Class Members.

E. Defendant Failed to Comply with Federal Trade Commission Guidelines and Industry Standards for Cybersecurity.

100. Data breaches are preventable.[37] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[38] "Organizations that collect, use, store, and share sensitive

[37] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.
[38] *Id.* at 17.

personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[39]

101. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[40]

102. Here, many failures laid the groundwork for the Data Breach.

103. The FTC has published guidelines that establish reasonable data security practices for businesses.[41]

104. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[42]

105. The FTC guidelines establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems.[43]

106. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

[39] *Id.* at 28.
[40] *Id.*
[41] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[42] *Id.*
[43] *Id.*

hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[44]

107. According to information and belief, Defendant failed to follow reasonable and necessary industry standards to prevent the Breach, including the FTC's guidelines.

108. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

109. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[45]

110. To prevent and detect the attack here, Defendant could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

- Implemented an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enabled strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

---

[44] *Id.*

[45] *See How to Protect Your Networks from RANSOMWARE*, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Managed the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configured access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disabled macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implemented Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.

- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[46]

111. According to information and belief, Defendant failed to do any of the above.

112. To prevent and detect ransomware attacks, Defendant could and should have recommended its employees, as recommended by the United States Cybersecurity & Infrastructure Security Agency, take the following measures:

- **Updated and patched your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Used caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

[46] *Id.* at 3–4.

- **Opened email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Kept your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verified email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Used and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[47]

[47] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

113. In addition, to prevent and detect the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
- **Thoroughly investigate and remediate alerts.**
  - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
  - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**
  - Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
    - Utilize Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications[48]

114. Given that Defendant was storing the Private Information of thousands of individuals, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks. However, Defendant failed to do so because an unknown third-party was able to gain access to Defendant's inadequately secured network and systems and exfiltrate the sensitive Private Information of Plaintiffs and Class Members.

115. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[49]

116. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.[50]

117. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business

[48] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT Intelligence (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.
[49] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.
[50] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[51] Rather than following this basic standard of care, Defendant kept thousands of current and former employees' unencrypted Private Information on its inadequately secured systems indefinitely.

118. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a Breach.

119. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep the Private Information private and secure, Defendant failed to take appropriate steps, as recommended by the FTC, to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

120. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation and encryption of all Private Information—which Defendant negligently failed to do.

121. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices—but Defendant negligently did no such thing.

[51] *Id.* at 6.

F. Defendant Had a Duty to Plaintiffs and Class Members to Safeguard their Private Information from Unauthorized Disclosure.

122. By collecting, accepting, and storing Plaintiffs' and Class Members' Private Information in its systems and network, Defendant owed a duty of care to Plaintiffs and Class Members to adequately and reasonably secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees on cybersecurity, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when Defendant became aware that their Private Information may have been compromised.

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

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

G. Common Injuries and Damages.

125. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft and misuse of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

H. Loss of Time to Mitigate the Risks of Fraud and Identity Theft.

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

127. Due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm. Identity theft protection and credit monitoring services are reasonable and necessary for Plaintiffs and Class Members to protect themselves against fraud and identity theft. Plaintiffs and Class Members will have to pay for these services for the rest of their lives now that their Private Information has been accessed and exposed in Defendant's Breach.

128. Plaintiffs and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing freezes and alerts with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing

passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

129. These efforts are consistent with the U.S. Government Accountability Office, which released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record.[52]

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

I. Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

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

132. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes— e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

[52] See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf. (last visited Oct. 8, 2026).

133. By accessing and obtaining the PII in the Breach, hackers have everything they need to commit fraud and identity theft.

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

135. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[53]

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

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

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

[53] Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Feb. 11, 2025).

J. Loss of the Benefit of the Bargain

139. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to directly or indirectly provide their Private Information to Defendant, Plaintiffs and other reasonable consumers understood and expected that in exchange, Defendant would implement necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

K. Plaintiffs' Individual Experience

Plaintiff David Reed

140. Plaintiff Reed is a former employee of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and bank account information, to Defendant as part of Defendant's business practices. Plaintiff Reed was employed by Defendant between approximately May 2019 through September 2021.

141. Plaintiff Reed received a Notice Letter from the Defendant informing him that at least his name, Social Security number, date of birth, salary, bank account information for direct deposit, home address, and, possibly, passport number, were involved in the Data Breach.

142. Plaintiff Reed entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

143. By soliciting and accepting Plaintiff Reed's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

144. Plaintiff Reed would not have provided his Private Information to Defendant had

he known it would be kept using inadequate data security and vulnerable to a cyberattack.

145. Upon information and belief, Defendant was in possession of Plaintiffs Reed's Private Information before, during, and after the Data Breach.

146. As a result, Plaintiff Reed was injured by Defendant's Data Breach.

147. In response to the Data Breach, upon information and belief, Plaintiff Reed made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. Plaintiff Reed estimates he has already spent at least 10 hours responding to the Data Breach.

148. Plaintiff Reed will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

149. Plaintiff Reed places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Reed entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

150. Because of the Data Breach, there is no doubt Plaintiffs Reed's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web. On September 19, 2026, Plaintiff Reed received a dark web alert from IDShield (which he has through his current employer). The dark web alert notified Plaintiff Reed that on July 29, 2026, his Turner email address was the affected email address associated with the dark web leak. He also received

a second alert from IDShield saying the event date was 8/11/26. As such, Plaintiff Reed and the Class are at an imminent risk of identity theft and fraud.

151. After the Data Breach, Plaintiff Reed suffered from a significant increase in spam scams and spam communications. Specifically, since the Data Breach, Plaintiff Reed has received an increase in spam calls, all related to phishing attempts to obtain additional personal information from Plaintiff Reed and the sale and marketing of goods and services that Plaintiff Reed did not request. Prior to the Data Breach, Plaintiff Reed did not experience this amount or type of spam communications. Defendant had in its possession Plaintiffs Reed's phone number at the time of the Breach. Plaintiff Reed attributes the increase in spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Reed's experience.

152. Plaintiff Reed has experienced fraud. Specifically, around August 2026, Plaintiff Reed noticed that his credit score had decreased and he checked his report. Plaintiff Reed noticed that a fraudulent Wells Fargo credit card was opened using his information on July 9, 2026, which was negatively impacting his credit score. Plaintiff Reed then called Wells Fargo about the fraudulent account, and the bank immediately closed the account. The Wells Fargo fraudulent account incident dropped his credit score by around 50 points, and his score has not yet recovered to pre-fraud levels. Further, on September 19, 2026, Plaintiff Reed experienced an unauthorized login attempt to his Affirm account. Affirm notified Plaintiff Reed of the attempt via email on that date and that Affirm had blocked the attempt.

153. Plaintiff Reed suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

154. Plaintiff Reed suffered actual injury in the form of damages to and diminution in

the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

155. Due to Defendant's Breach, Plaintiff Reed will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Reed's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

156. Plaintiff Reed's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

157. Knowing that thieves intentionally targeted and accessed his Private Information, has caused Plaintiff Reed great anxiety beyond mere worry.

158. The Data Breach has caused Plaintiff Reed to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

159. Plaintiff Reed has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

160. As a direct and traceable result of the Data Breach, Plaintiff Reed suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not

adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Reed; and (vii) other economic and non-economic harm.

161. Plaintiff Reed has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

162. Plaintiff Reed has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Reed's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Jaden Dias

163. Plaintiff Dias is a former employee of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and bank account information, to Defendant as part of Defendant's business practices. Plaintiff Dias was employed by Defendant between approximately June and August of 2024.

164. Plaintiff Dias received a Notice Letter from the Defendant informing him that at least his name, Social Security number, Social Insurance Number, date of birth, salary, bank account information used for direct deposits, and home address were involved in the Data Breach.

165. Plaintiff Dias entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure

from unauthorized access.

166. By soliciting and accepting Plaintiff Dias's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

167. Plaintiff Dias would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

168. Upon information and belief, Defendant was in possession of Plaintiffs Dias's Private Information before, during, and after the Data Breach.

169. As a result, Plaintiff Dias was injured by Defendant's Data Breach.

170. In response to the Data Breach, upon information and belief, Plaintiff Dias made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. Plaintiff Dias estimates he has already spent at least 3 hours responding to the Data Breach.

171. Plaintiff Dias will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

172. Plaintiff Dias places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Dias entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

173. Because of the Data Breach, there is no doubt Plaintiffs Dias's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of

cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web.

174. After the Data Breach, Plaintiff Dias suffered from a significant increase in spam communications. Specifically, since the Data Breach, Plaintiff Dias has received an increase in spam calls and text messages. Prior to the Data Breach, Plaintiff Dias did not experience this amount or type of spam communications. Defendant had in its possession Plaintiffs Dias's phone number at the time of the Breach. Plaintiff Dias attributes the increase in spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Dias's experience.

175. Plaintiff Dias suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

176. Plaintiff Dias suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

177. Due to Defendant's Breach, Plaintiff Dias will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Dias's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

178. Plaintiff Dias's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

179. Knowing that thieves intentionally targeted and accessed his Private Information,

has caused Plaintiff Dias great anxiety beyond mere worry.

180. The Data Breach has caused Plaintiff Dias to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

181. Plaintiff Dias has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

182. As a direct and traceable result of the Data Breach, Plaintiff Dias suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Dias; and (vii) other economic and non-economic harm.

183. Plaintiff Dias has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

184. Plaintiff Dias has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Dias's Private

Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff George R. Booth

185. Plaintiff Booth is a former employee of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and bank account information, to Defendant as part of Defendant's business practices. Plaintiff Booth was employed by Defendant around 2021.

186. Plaintiff Booth received a Notice Letter from the Defendant informing him that at least his name, Social Security number, date of birth, salary, bank account information for direct deposit, home address, and, possibly, passport number, were involved in the Data Breach.

187. Plaintiff Booth entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

188. By soliciting and accepting Plaintiff Booth's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

189. Plaintiff Booth would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

190. Upon information and belief, Defendant was in possession of Plaintiffs Booth's Private Information before, during, and after the Data Breach.

191. As a result, Plaintiff Booth was injured by Defendant's Data Breach.

192. In response to the Data Breach, upon information and belief, Plaintiff Booth made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. Plaintiff Booth estimates he has already spent at least 10 hours

responding to the Data Breach.

193. Plaintiff Booth will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

194. Plaintiff Booth places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Booth entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

195. Because of the Data Breach, there is no doubt Plaintiffs Booth's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web. As such, Plaintiff Booth and the Class are at an imminent risk of identity theft and fraud.

196. After the Data Breach, Plaintiff Booth suffered from a significant increase is spam scams and spam communications. Specifically, since the Data Breach, Plaintiff Booth has received 4-5 spam calls per day related to phishing attempts to obtain additional personal information from Plaintiff Booth and the sale and marketing of goods and services that Plaintiff Booth did not request. Prior to the Data Breach, Plaintiff Booth did not experience this amount or type of spam communications. Defendant had in its possession Plaintiffs Booth's phone number at the time of the Breach. Plaintiff Booth attributes the increase in spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Booth's experience.

197. Plaintiff Booth has experienced attempted fraud. Specifically, on or around August

and September of 2026, an unknown actor attempted to access Plaintiff's financial accounts and/or services connected with those accounts. Upon information and belief, Defendant had Plaintiff Booth's financial account information at the time of the Breach. Plaintiff Booth attributes this attempted fraud based on temporal proximity and the fact that this type of attempted fraud is atypical in Plaintiff Booth's experience.

198. Plaintiff Booth suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

199. Plaintiff Booth suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

200. Due to Defendant's Breach, Plaintiff Booth will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Booth's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

201. Plaintiff Booth's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

202. Knowing that thieves intentionally targeted and accessed his Private Information, has caused Plaintiff Booth great anxiety beyond mere worry.

203. The Data Breach has caused Plaintiff Booth to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private

Information was accessed and/or acquired by criminals as a result of the Data Breach.

204. Plaintiff Booth has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

205. As a direct and traceable result of the Data Breach, Plaintiff Booth suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Booth; and (vii) other economic and non-economic harm.

206. Plaintiff Booth has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

207. Plaintiff Booth has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Booth's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Johnny Hewett

208. Plaintiff Hewett is a former employee of Defendant and was required to provide his

Private Information including name, date of birth, Social Security number, phone number and bank account information, to Defendant as part of Defendant's business practices.

209. Plaintiff Hewett received Notice from the Defendant via his employee email account, informing him that his Private Information was involved in the Data Breach.

210. Plaintiff Hewett entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

211. By soliciting and accepting Plaintiff Hewett's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

212. Plaintiff Hewett would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

213. Upon information and belief, Defendant was in possession of Plaintiff Hewett's Private Information before, during and after the Data Breach.

214. As a result, Plaintiff Hewett was injured by Defendant's Data Breach.

215. In response to the Data Breach, upon information and belief, Plaintiff Hewett made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, reviewing his credit reports and notifying his bank and credit card companies about the Data Breach. Plaintiff Hewett estimates he has already spent at least 3 hours responding to the Data Breach.

216. Plaintiff Hewett will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

217. Plaintiff Hewett places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Hewett entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

218. Because of the Data Breach, there is no doubt Plaintiff Hewett's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout Kings, is to steal data they can exploit by selling on the dark web. As such, Plaintiff Hewett and the Class are at an imminent risk of identity theft and fraud.

219. After the Data Breach, Plaintiff Hewett suffered from a significant increase in spam and scam communications. Defendant had in its possession Plaintiffs Hewett's phone number at the time of the Breach. Plaintiff Hewett attributes the increase in spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Hewett's experience.

220. Plaintiff Hewett suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

221. Plaintiff Hewett suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

222. Due to Defendant's Breach, Plaintiff Hewett will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a

consequence of Defendant's breach of duty to maintain Plaintiff Hewett's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

223. Plaintiff Hewett's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

224. Knowing that thieves intentionally targeted and accessed his Private Information, has caused Plaintiff Hewett great anxiety beyond mere worry.

225. The Data Breach has caused Plaintiff Hewett to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

226. Plaintiff Hewett has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

227. As a direct and traceable result of the Data Breach, Plaintiff Hewett suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Booth; and (vii) other economic and non-economic harm.

228. Plaintiff Hewett has been and will continue to be at a heightened and substantial

risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

229. Plaintiff Hewett has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Hewett's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Joshua Donald

230. Plaintiff Donald is a former intern of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and bank account information, to Defendant as part of Defendant's business practices. Plaintiff Donald interned with Defendant's company in the summer of 2016.

231. Plaintiff Donald received a Notice Letter from the Defendant informing him that at least his name, Social Security number, date of birth, salary, bank account information for direct deposit, home address, and, possibly, passport number, were involved in the Data Breach.

232. Plaintiff Donald entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

233. By soliciting and accepting Plaintiff Donald's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

234. Plaintiff Donald would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

235. Upon information and belief, Defendant was in possession of Plaintiffs Donald's

Private Information before, during, and after the Data Breach.

236. As a result, Plaintiff Donald was injured by Defendant's Data Breach.

237. In response to the Data Breach, upon information and belief, Plaintiff Donald made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. Plaintiff Donald estimates he has already spent at least 2 hours responding to the Data Breach.

238. Plaintiff Donald will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

239. Plaintiff Donald places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Donald entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

240. Because of the Data Breach, there is no doubt Plaintiffs Donald's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web. As such, Plaintiff Donald and the Class are at an imminent risk of identity theft and fraud.

241. After the Data Breach, Plaintiff Donald suffered from a significant increase is spam scams and spam communications. Specifically, since the Data Breach, Plaintiff Donald has received 3 spam calls, 2 spam emails, and 2 pam texts per week all related to phishing attempts to

obtain additional personal information from Plaintiff Donald, delivery of unknown UPS packages, quotes for roofing services, unpaid tolls that Plaintiff Donald does not recognize, and the sale and marketing of goods and services that Plaintiff Donald did not request. Prior to the Data Breach, Plaintiff Donald did not experience this amount or type of spam communications. Defendant had in its possession Plaintiffs Donald's phone number and email address at the time of the Breach. Plaintiff Donald attributes the increase in spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Donald's experience.

242. Plaintiff Donald suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

243. Plaintiff Donald suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

244. Due to Defendant's Breach, Plaintiff Donald will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Donald's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

245. Plaintiff Donald's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

246. Knowing that thieves intentionally targeted and accessed his Private Information,

has caused Plaintiff Donald great anxiety beyond mere worry.

247. The Data Breach has caused Plaintiff Donald to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

248. Plaintiff Donald has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

249. As a direct and traceable result of the Data Breach, Plaintiff Donald suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Donald; and (vii) other economic and non-economic harm.

250. Plaintiff Donald has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

251. Plaintiff Donald has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Donald's Private

Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Louis Martinelli

252. Plaintiff Martinelli is a former employee of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and bank account information, to Defendant as part of Defendant's business practices. Plaintiff Martinelli was employed by Defendant between March 2021 through January 2026.

253. Plaintiff Martinelli received a Notice Letter from the Defendant informing him that at least his name, Social Security number, date of birth, salary, bank account information for direct deposit, home address, and, possibly, passport number, were involved in the Data Breach.

254. Plaintiff Martinelli entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

255. By soliciting and accepting Plaintiff Martinelli's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

256. Plaintiff Martinelli would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

257. Upon information and belief, Defendant was in possession of Plaintiffs Martinelli's Private Information before, during, and after the Data Breach.

258. As a result, Plaintiff Martinelli was injured by Defendant's Data Breach.

259. In response to the Data Breach, upon information and belief, Plaintiff Martinelli made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, mitigating fraud activity with his bank, filtering through spam communications, and reviewing his

credit reports. Plaintiff Martinelli estimates he has already spent at least 40 hours responding to the Data Breach.

260. Plaintiff Martinelli will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

261. Plaintiff Martinelli places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Martinelli entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

262. Because of the Data Breach, there is no doubt Plaintiffs Martinelli's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web. As such, Plaintiff Martinelli and the Class are at an imminent risk of identity theft and fraud.

263. After the Data Breach, Plaintiff Martinelli suffered from a significant increase is spam scams and spam communications. Specifically, since the Data Breach, Plaintiff Martinelli has received spam calls and spam emails, all related to phishing attempts to obtain additional personal information from Plaintiff Martinelli and the sale and marketing of goods and services that Plaintiff Martinelli did not request. Plaintiff Martinelli has received emails regarding account setups for fraudulent accounts with Staples and Samsung. On August 25, 2026, and September 1, 2026, Plaintiff Martinelli received emails from Staples and Samsung informing Plaintiff Martinelli of a summary of unrecognized orders and payment is immediately needed to process such

fraudulent orders. Prior to the Data Breach, Plaintiff Martinelli did not experience this type of spam communications. Defendant had in its possession Plaintiffs Martinelli's phone number and email address at the time of the Breach. Plaintiff Martinelli attributes these spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Martinelli's experience.

264. Plaintiff Martinelli has experienced fraud. Specifically, after receiving a Notice Letter from Defendant on August 2026, Plaintiff checked his bank account and noticed that between the months of August and September of 2026, there were numerous fraudulent attempts to withdraw money from ATM machines using Plaintiff Martinelli's debit card. Plaintiff Martinelli provided his debit card information to Defendant in connection with his employment and Defendant had such information in its possession at the time of the Breach.

265. On August 25, 2026 and September 1, 2026, Plaintiff received emails from Staples and Samsung regarding summary orders and payment requests to process such order which Plaintiff Martinelli did not place.

266. On September 20, 2026, Plaintiff Martinelli received an email from Crypto.com alerting Plaintiff Martinelli of a sign-in attempt on Plaintiff's account. The email requested Plaintiff Martinelli to confirm that he was the individual attempting to sign-in. Defendant had in its possession Plaintiff Martinelli's email address at the time of the Breach.

267. Lastly, on September 1, 2026, NordVPN notified Plaintiff Martinelli of two attempts to use his personal information to make purchases with vendor MSG Sport which Plaintiff did not make.

268. In response to the above fraudulent activity, Plaintiff Martinelli contacted his bank to freeze his account and withdraw his funds, causing Plaintiff Martinelli to spend additional time

to mitigate the above fraud activity and placing Plaintiff Martinelli at risk of having his bank account closed. As a result of the above fraud activity, Plaintiff Martinelli's credit score dropped from his original 800+ score.

269. Plaintiff Martinelli suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

270. Plaintiff Martinelli suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

271. Due to Defendant's Breach, Plaintiff Martinelli will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Martinelli's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

272. Plaintiff Martinelli's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

273. Knowing that thieves intentionally targeted and accessed his Private Information, has caused Plaintiff Martinelli great anxiety beyond mere worry.

274. The Data Breach has caused Plaintiff Martinelli to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

275. Plaintiff Martinelli has never knowingly transmitted unencrypted Private

Information over the internet or any other unsecured source.

276. As a direct and traceable result of the Data Breach, Plaintiff Martinelli suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Martinelli; and (vii) other economic and non-economic harm.

277. Plaintiff Martinelli has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

278. Plaintiff Martinelli has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Martinelli's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Bill Bishop

279. Plaintiff Bishop is a former employee of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and

bank account information, to Defendant as part of Defendant's business practices. Plaintiff Bishop was employed by Defendant between approximately 2004 through 2023.

280. Plaintiff Bishop received a Notice Letter from the Defendant informing him that at least his name, Social Security number, date of birth, salary, bank account information for direct deposit, home address, and, possibly, passport number, were involved in the Data Breach.

281. Plaintiff Bishop entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

282. By soliciting and accepting Plaintiff Bishop's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

283. Plaintiff Bishop would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

284. Upon information and belief, Defendant was in possession of Plaintiffs Bishop's Private Information before, during, and after the Data Breach.

285. As a result, Plaintiff Bishop was injured by Defendant's Data Breach.

286. In response to the Data Breach, upon information and belief, Plaintiff Bishop made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. Plaintiff Bishop estimates he has already spent at least 17 hours responding to the Data Breach.

287. Plaintiff Bishop will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

288. Plaintiff Bishop places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Bishop entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

289. Because of the Data Breach, there is no doubt Plaintiffs Bishop's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web.

290. Plaintiff Bishop has experienced Fraud. On September 11, 2026, Plaintiff Bishop was the victim of a phone scam. A person called him purporting to be an agent of the Federal Bureau of Investigation ("FBI") and deceived Plaintiff Bishop into wiring approximately $9,800. Plaintiff Bishop spent approximately 9 hours working to remedy this fraud to have his money reimbursed. As such, Plaintiff Bishop and the Class are at an imminent risk of identity theft and fraud.

291. Plaintiff Bishop suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

292. Plaintiff Bishop suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

293. Due to Defendant's Breach, Plaintiff Bishop will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been

published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Bishop's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

294. Plaintiff Bishop's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

295. Knowing that thieves intentionally targeted and accessed his Private Information, has caused Plaintiff Bishop great anxiety beyond mere worry.

296. The Data Breach has caused Plaintiff Bishop to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

297. Plaintiff Bishop has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

298. As a direct and traceable result of the Data Breach, Plaintiff Bishop suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Bishop; and (vii) other economic and non-economic harm.

299. Plaintiff Bishop has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

300. Plaintiff Bishop has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs Bishop's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Mustafa Arsiwala

301. Plaintiff Ariswala is a former employee of Defendant and was required to provide his Private Information, including name, date of birth, Social Security number, phone number, and bank account information, to Defendant as part of Defendant's business practices. Plaintiff Ariswala was employed by Defendant between approximately February through July 2026.

302. Plaintiff Ariswala received a Notice Letter from the Defendant informing him that at least his name, Social Security number, date of birth, salary, bank account information for direct deposit, home address, and, possibly, passport number, were involved in the Data Breach.

303. Plaintiff Ariswala entrusted his Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

304. By soliciting and accepting Plaintiff Ariswala's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

305. Plaintiff Ariswala would not have provided his Private Information to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

306. Upon information and belief, Defendant was in possession of Plaintiffs Ariswala's Private Information before, during, and after the Data Breach.

307. As a result, Plaintiff Ariswala was injured by Defendant's Data Breach.

308. In response to the Data Breach, upon information and belief, Plaintiff Ariswala made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. Plaintiff Ariswala estimates he has already spent at least 15 hours responding to the Data Breach.

309. Plaintiff Ariswala will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent which has been lost forever and cannot be recaptured.

310. Plaintiff Ariswala places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Ariswala entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

311. Because of the Data Breach, there is no doubt Plaintiffs Ariswala's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals, like Payout King, is to steal data they can exploit by selling on the dark web. Plaintiff Ariswala has received several dark web alerts from IDShield. The dark web alerts notified Plaintiff Ariswala that his email address and phone numbers were found on the dark web. As such, Plaintiff Ariswala and the Class are at an imminent risk of identity theft and fraud.

312. After the Data Breach, Plaintiff Ariswala suffered from a significant increase in

spam scams and spam communications. Specifically, since the Data Breach, Plaintiff Ariswala has received an increase in spam calls, all related to phishing attempts to obtain additional personal information from Plaintiff Ariswala and the sale and marketing of goods and services that Plaintiff Ariswala did not request. Prior to the Data Breach, Plaintiff Ariswala did not experience this amount or type of spam communications. Defendant had in its possession Plaintiffs Ariswala's phone number at the time of the Breach. Plaintiff Ariswala attributes the increase in spam communications to the Data Breach based on temporal proximity, the careful handling of his Private Information, and the fact that these spam communications are atypical in Plaintiff Ariswala's experience.

313. Plaintiff Ariswala suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

314. Plaintiff Ariswala suffered actual injury in the form of damages to and diminution in the value of his Private Information. PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

315. Due to Defendant's Breach, Plaintiff Ariswala will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, his information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff Ariswala's highly sensitive Private Information, including his Social Security number, secure and protected against unauthorized disclosure.

316. Plaintiff Ariswala's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

317. Knowing that thieves intentionally targeted and accessed his Private Information, has caused Plaintiff Ariswala great anxiety beyond mere worry.

318. The Data Breach has caused Plaintiff Ariswala to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying him of the fact that his Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

319. Plaintiff Ariswala has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

320. As a direct and traceable result of the Data Breach, Plaintiff Ariswala suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (ii) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of his bargain because Defendant did not adequately protect his Private Information; (iv) emotional distress because identity thieves now possess his Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (vi) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Ariswala; and (vii) other economic and non-economic harm.

321. Plaintiff Ariswala has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

322. Plaintiff Ariswala has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and

safeguarded from future data breaches. Absent Court intervention, Plaintiffs Ariswala's Private Information will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

323. Plaintiffs incorporate by reference all preceding factual paragraphs as if fully restated here.

324. Plaintiffs bring this action against Defendant individually and on behalf of all others similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a Nationwide Class and/or State Subclass (collectively, the "Class") defined as follows:

> **Nationwide Class:** All individuals residing in the United States whose PII was accessed and/or compromised as a result of the Data Breach, including all persons that were sent a Notice Letter.
>
> **New York Subclass**: All individuals domiciled in New York whose PII was accessed and/or compromised as a result of the Data Breach, including all individuals domiciled in New York that were sent a Notice Letter

325. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and their judicial staff members. Plaintiffs reserve the right to amend or modify the above Class definition or to propose subclasses in subsequent pleadings and motions for class certification.

326. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

327. The proposed Class meets the requirements of FRCP 23.

328. **Numerosity.** Class Members are so numerous that joining all members is impracticable. Upon information and belief, the Class consists of thousands of individuals affected by the Data Breach. Each Class Member is apparently identifiable within Defendant's records.

329. **Typicality.** Plaintiffs' claims are typical of the claims of the Class because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs and all members of the Class were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that gives rise to the claims of all Class Members.

330. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class. Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation, and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and his counsel.

331. **Superiority**. A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the Class to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents 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 benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

332. **Commonality and Predominance.** Defendant engaged in a common course of conduct toward Plaintiffs and Class Members, in that Plaintiffs' and Class Members' Private Information was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their Private Information;

c. Whether Defendant breached its duty to Plaintiffs and Class Members to adequately protect their Private Information;

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

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

g. Whether Defendant knew or should have known that its computer and network security systems, or the computer and network security systems of its vendors, were vulnerable to cyberattacks;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

i. Whether Defendant was negligent in permitting unencrypted Private Information belonging to thousands of individuals to be stored within their network;

j. Whether Defendant was negligent in failing to adhere to reasonable data retention policies;

k. Whether Defendant breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their Private Information;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class Members;

m. Whether Defendant should have discovered the Data Breach sooner;

n. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

o. Whether Defendant continues to breach duties owed to Plaintiffs and the Class;

p. Whether Plaintiffs and the Class suffered injuries as a proximate result of Defendant's negligent actions or failures to act;

q. Whether Defendant was negligent in selecting, supervising, and/or monitoring vendors;

r. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

s. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

333. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach

334. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed are representatives of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

335. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

336. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

337. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

338. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

339. Plaintiffs re-allege and incorporate by reference paragraphs 1-338 as if fully restated here.

340. Defendant knowingly solicited, collected, stored, and maintained the Private Information of Plaintiffs for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

341. Upon accepting and storing Plaintiffs' and Class Members' Private Information on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class

Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information from unauthorized access and disclosure.

342. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Private Information.

343. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

344. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

345. Defendant had full knowledge of the sensitivity of the Private Information in its possession and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully accessed or disclosed. Plaintiffs and Class Members were therefore the foreseeable victims of any inadequate data security practices.

346. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class directly or indirectly entrusted Defendant with their confidential Private Information, a mandatory step in obtaining services and/or employment from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's privacy practices, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered Private Information as part of its business and was solely

responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a resulting data breach.

347. Defendant's duty to implement and maintain reasonable data security practices arose as a result of the special relationship that exists between Defendant and consumers, which is recognized by laws and regulations, including, but not limited to, the FTC Act and common law.

348. Defendant was in a superior position to ensure its data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

349. Defendant knew Plaintiffs and Class Members relied on it to protect their Private Information. Plaintiffs and Class Members were not in a position to assess the data security practices used by Defendant. Because they had no means to identify Defendant's security deficiencies, Plaintiffs and Class Members had no opportunity to safeguard their Private Information from cybercriminals. Defendant exercised control over the Private Information stored on its systems and networks; accordingly, Defendant was best positioned and most capable of preventing the harms caused by the Data Breach.

350. Defendant was aware, or should have been aware, of the fact that cybercriminals routinely target entities storing PII through cyberattacks in an attempt to steal valuable Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

351. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and Class

Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

352. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to such risk, or defeats protections put in place to guard against that risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

353. Defendant had a duty to implement and maintain reasonable data security practices pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect sensitive and confidential data.

354. 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 PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

355. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information as part of their regular business, which affects commerce.

356. Defendant violated the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and by failing to comply with applicable industry standards, as described herein.

357. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to implement and maintain fair, reasonable, and adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt

notice of the Data Breach without unreasonable delay.

358. Defendant's multiple failures to comply with applicable laws and regulations constitute negligence *per se*.

359. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

360. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, like Defendant, that fail to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiffs and the Class.

361. Defendant breached its duties to Plaintiffs and the Class by delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

362. Defendant's violations of the FTC Act constitute negligence *per se*.

363. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

364. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

365. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information.

366. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' Private Information;

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

c. Failing to ensure its email systems had plans in place to maintain reasonable data security safeguards;

d. Failing to implement and maintain adequate mitigation policies and procedures;

e. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

f. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised; and

g. Failing to timely notify Plaintiffs and Class Members about the Data Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

367. Defendant's willful failure to abide by its duties to Plaintiffs and Class Members was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

368. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would result in injury to Plaintiffs and Class Members.

369. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry.

370. Defendant had a common law duty to prevent foreseeable harm to others. Plaintiffs and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting

and storing the Private Information of Plaintiffs and the Class, the critical importance of adequately safeguarding that Private Information, and the necessity of encrypting Private Information stored on Defendant's systems. It was foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

371. Defendant's conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiffs' and the Class's Private Information, including basic encryption techniques available to Defendant.

372. As a direct and proximate result of Defendant's negligent conduct, including, but not limited to, its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

373. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

374. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Private Information and mitigate the impact of the Data Breach.

375. Plaintiffs and Class Members could have taken actions earlier had they been timely notified of the Data Breach. Yet, Defendant delayed in noticing Plaintiffs and Class Members of the Breach.

376. Plaintiffs and Class Members could have enrolled in credit monitoring, instituted credit freezes, and changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

377. Plaintiffs and Class Members suffered harm from Defendant's delay in notifying them of the Data Breach.

378. As a direct and proximate result of Defendant's conduct, including, but not limited to, Defendant's failure to implement and maintain reasonable data security practices and procedures, Plaintiffs and Class Members have suffered or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to address and 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 fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk 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 the Private

Information in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

379. The damages Plaintiffs and the Class have suffered and will suffer (as alleged above) were and are the direct and proximate result of Defendant's negligent conduct.

380. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered cognizable injuries and are entitled to actual, consequential, and nominal damages and injunctive relief to be determined at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

381. Plaintiffs re-allege and incorporate by reference paragraphs 1-338 as if fully restated here.

382. Plaintiffs and Class Members were required to provide their Private Information to Defendant, directly or indirectly, in order to receive services and/or employment. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services and employment.

383. Defendant solicited and accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services and/or employment to Plaintiffs and Class Members.

384. In delivering, directly or indirectly, their Private Information to Defendant and paying for services or receiving employment, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard their Private Information.

385. Plaintiffs and Class Members reasonably expected that the Private Information they entrusted to Defendant, in order to receive services or as a condition of their employment, would remain confidential and would not be shared or disclosed to criminal third parties.

386. At the time Defendant acquired the Private Information of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the Private Information and not take unjustified risks when storing the Private Information.

387. Plaintiffs and Defendant had a mutual understanding that Defendant would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiffs' and Class Members' sensitive Private Information. Plaintiffs and Defendant also shared an expectation and understanding that Defendant would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in its possession and control.

388. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and Class Members' Private Information, Defendant had a duty to safeguard the Private Information in its possession through the use of reasonable data security practices.

389. When Plaintiffs and Class Members paid money and provided their Private Information to Defendant, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Defendant.

390. Defendant entered into implied contracts with Plaintiffs and the Class under which Defendant agreed to comply with its statutory and common law duties to safeguard and protect Plaintiffs' and Class Members' Private Information and to timely notify Plaintiffs and Class Members of a data breach. In exchange, Plaintiffs and Class Members provided their Private Information to Defendant and paid money to Defendant, directly or indirectly, which a portion was

to ensure that Defendant maintained adequate security measures to protect the PII and PHI of Plaintiffs and the Class.

391. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under Section 5 of the FTC Act and other state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

392. The implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to Private Information protect the confidentiality of that information; (ii) taking steps to ensure that Private Information in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized business purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (v) applying or requiring proper encryption of the Private Information; (vi) requiring multifactor authentication for access to the Private Information; and (vii) other steps necessary to protect against foreseeable data breaches.

393. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of such implied contracts.

394. Defendant recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance to Plaintiffs and Class Members.

395. Had Defendant disclosed to Plaintiffs and Class Members that it did not have adequate data security practices to secure their Private Information, Plaintiffs and Class Members would not have provided their Private Information to Defendant.

396. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

397. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

398. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

399. Plaintiffs and the Class have suffered injuries as described above, and are entitled to actual, consequential, and nominal damages to be determined at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

400. Plaintiffs re-allege and incorporate by reference paragraphs 1-338 as if fully restated here.

401. Plaintiffs allege this claim in the alternative to their breach of implied contract claim.

402. Plaintiffs and the Class provided their Private Information to Defendant in order to receive services or employment.

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

404. By conferring their Private Information to Defendant, Plaintiffs and Class Members reasonably understood Defendant would be responsible for securing their Private Information from unauthorized access and disclosure.

405. Upon information and belief, Defendant funds its data security measures entirely from their general revenue, including revenues made through the labor of Plaintiffs and Class Members.

406. As such, a portion of the revenue generated from the labor of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the revenue generated that is allocated to data security is known to Defendant.

407. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

408. Protecting the Private Information of Plaintiffs and Class Members is integral to Defendant's business. Without their Private Information, Defendant would be unable to provide services comprising Defendant's core business.

409. Plaintiffs' and Class Members' Private Information have monetary value.

410. Plaintiffs and Class Members directly conferred a monetary benefit on Defendant by supplying their Private Information, from which Defendant derives its business, and which should have been protected with adequate data security.

411. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiffs and the Class. Defendant profited from these transactions and used Plaintiffs' and Class Members' Private Information for business purposes.

412. Indeed, Plaintiffs and Class Members who were employees of Defendant provided their labor to Defendant and therefore conferred a benefit unto Defendant.

413. Defendant appreciated that a monetary benefit was being conferred upon them by Plaintiffs and Class Members and accepted that monetary benefit.

414. Under the facts and circumstances outlined above, however, it is inequitable for Defendant to retain that benefit without payment of the value thereof.

415. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

416. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits to the detriment and at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

417. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

418. Defendant acquired Plaintiffs' and Class Members' Private Information through inequitable means in that they failed to disclose their inadequate data security practices, as previously alleged.

419. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have allowed Defendant to collect their Private Information.

420. Plaintiffs and Class Members have no adequate remedy at law.

421. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including, but not limited to: (i) actual identity theft and fraud; (ii) loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (v) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, effort and time spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk 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 the Private Information in their continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

423. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that it unjustly received.

FOURTH CAUSE OF ACTION
VIOLATION OF NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law § 349, *et seq*.
(On Behalf of Plaintiffs Booth, Martinelli, and the New York Subclass)

424. Plaintiffs Booth and Martinelli ("New York Plaintiffs") repeat and re-allege the preceding factual allegations, as if fully set forth herein.

425. New York Plaintiffs bring the following claim against Defendant on behalf of themselves and the New York Subclass.

426. New York General Business Law § 349(a) states, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

427. Defendant is a "person, firm, corporation or association or agent or employee thereof" within the meaning of N.Y. Gen. Bus. Law § 349(b).

428. At all relevant times, Defendant was engaged in "business," "trade," or "commerce" within the meaning of N.Y. Gen. Bus. Law § 349(a).

429. New York Plaintiffs and New York Subclass Members are "persons" within the meaning of N.Y. Gen. Bus. Law § 349(h).

430. At all relevant times, Defendant, with its headquarters and offices in New York, engaged in transactions affecting trade or commerce and furnishing services in New York including, but not limited to, the responsibility for overseeing or contributing to the protocols for properly safeguarding New York Plaintiffs' and New York Subclass Members' Private Information.

431. More specifically, Defendant engaged in deceptive acts and practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in New York, in violation of N.Y. Gen. Bus. Law § 349, including by:

a. failing to implement and maintain reasonable security and privacy measures to protect New York Plaintiffs' Private Information, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' Private Information, including, but not limited to, duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. failing to timely and adequately notify New York Plaintiffs of the Data Breach;

e. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure New York Plaintiffs' Private Information; and

f. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' Private Information, including, but not limited to, duties imposed by the FTC Act, 15 U.S.C. § 45.

432. Had New York Plaintiffs and New York Subclass Members been aware that Defendant did not maintain adequate data security safeguards, New York Plaintiffs and New York Subclass Members would not have provided their Private Information to Defendant.

433. As a direct and proximate cause of Defendant's unfair and deceptive trade practices, New York Plaintiffs and New York Subclass Members were damaged because: (a) they face a substantially increased risk of identity theft and other targeted misuse of their information—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (b) their Private Information was improperly disclosed to unauthorized individuals; (c) the confidentiality of their Private Information has been breached; (d) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (e) of lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (f) of loss of potential value of their Private Information; (g) of actual identity theft; (h) the continued risk 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 the Private Information in its possession; and (i) nominal damages.

434. Defendant's deceptive and unlawful acts and practices complained of herein affected consumers and the public interest and consumers at large, including at least thousands of New Yorkers affected by the Data Breach. Defendant's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including the New York Plaintiffs, regarding Defendant's data security measures and supervision of sensitive data entrusted to it.

435. Defendant's violations present a continuing risk to New York Plaintiffs and New York Subclass Members.

436. Pursuant to N.Y. Gen. Bus. Law § 349(h), New York Plaintiffs seek all monetary and non-monetary relief allowed by law, including damages on behalf of themselves and the other

New York Subclass Members in the amount of the greater of actual damages or $50 for each violation of N.Y. Gen. Bus. Law § 349. Because Defendant's conduct was committed willfully and knowingly, New York Plaintiffs and New York Subclass Members are entitled to recover up to three times their actual damages, up to $1,000, plus an award of reasonable attorney's fees.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on any and all issues raised in this Class Action Complaint so triable as of right.

Dated: October 16, 2026

Respectfully submitted,

/s/ Leanna A. Loginov
Leanna A. Loginov (NY 5894753)
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Telephone: (305) 479-2299
Email: lloginov@shamisgentile.com

Interim Lead Class Counsel for Plaintiffs

William B. Federman (NY 2215341)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Email: wbf@federmanlaw.com

Mark K. Svensson (NY 5894753)
MILBERG, PLLC
405 East 50th Street
New York, NY 10022
Telephone: (202) 975-0468
Email: msvensson@milberg.com

Sonal Jain (NY 5855275)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Telephone: (212) 532-1091
Email: sjain@sirillp.com

Tanner R. Hilton*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
101 Park Avenue Suite 1300, #16982799
Oklahoma City, OK 73102
Tel: (212) 532-1091
Email: tbean@sirillp.com

Email: thilton@sirillp.com

Israel David
Adam M. Harris
Mark A. Cianci*
ISRAEL DAVID LLC
60 Broad Street, Suite 2900
New York, NY 10004
Telephone: (212) 350-8850
Email: israel.david@davidllc.com
Email: adam.harris@davidllc.com
Email: mark.cianci@davidllc.com

Avi Mermelstein (NY 5184882)
ARENSON, DITTMAR & KARBAN
420 Lexington Avenue, Suite 1402
New York, NY 10170
Telephone: (212) 490-3600
Email: avi@adklawfirm.com

Mark T. Freeman*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, CA 94607
Telephone: (510) 891-9800
Email: mtf@colevannote.com

Raina C. Borrelli*
Cassandra P. Miller*
Andrew G. Gunem*
Carly M. Roman*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
2261 Market Street, Ste 22946
San Francisco, CA 94114
Telephone: (872) 263-1100
Email: raina@straussborrelli.com
Email: cmiller@straussborrelli.com
Email: bresch@straussborrelli.com
Email: agunem@straussborrelli.com
Email: croman@straussborrelli.com

Adam T. Savett*
WOLF POPPER LLP
570 Lexington Ave.

New York, NY 10022
Telephone: (212) 759-4600
Email: asavett@wolfpopper.com

Counsel for Plaintiffs and the Putative Class

** pro hac vice forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that on October 16, 2026, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ Leanna A. Loginov
Leanna A. Loginov