UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA

IN RE KRISPY KREME DATA SECURITY LITIGATION	Civil Action No.: 3:25-CV-00434 JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Fortesa Bobo, Lily Peace, Jalisa Bogan, Sebastian Schug, Tyreese Banks, Maria Alvarez, Augusta Burkes, Joseph DosReis, Andy Lavor as parent and legal guardian of his daughter I.L., Heather Robison, Duane Hopson, Kimberly Thompson, Suzzette Katzman, and Phillip McLaughlin (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this consolidated class action complaint against Defendant Krispy Kreme Doughnut Corporation ("Defendant"), and allege, upon personal knowledge as to their own actions and information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this consolidated class action against Defendant for its failure to properly secure and safeguard Plaintiffs and other similarly situated current and former employees' ("Class Members") sensitive information, including personally identifiable information ("PII") such as names, Social Security numbers, dates of birth, driver's licenses or state ID numbers, financial account information, financial account access information, credit or debit card information, credit or debit card security codes, usernames and passwords to a financial accounts, passport numbers, digital signatures, email addresses and passwords, biometric data, USCIS or

Alien Registration Number, and US military ID number; and protected health information ("PHI") including medical or health information, and health insurance information (collectively, "Private Information").

2. On or about November 29, 2024, the notorious ransomware group known as Play breached Defendant's network systems and targeted and stole Plaintiffs' and approximately 161,676 Class Members' confidential Private Information stored thereon (the "Data Breach").

3. Play then held Plaintiffs' and Class Members' stolen Private Information for ransom, threatening to post it on the Play dark web leak site if Defendant did not comply. Defendant did not pay Play's ransom demand, and the entire batch of Private Information stolen in the Data Breach is now published on Play's dark web leak page, for any bad actor to view, download, and use to further harm Plaintiffs and Class Members.

4. Defendant is multinational doughnut and coffee-house chain.

5. Plaintiffs and Class Members are Defendant's current and former employees, and as a condition of employment, entrusted Defendant with their sensitive Private Information

6. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information, or even to even encrypt or redact this highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its employees' sensitive data. The Play ransomware gang targeted and obtained Plaintiffs' and Class Members' Private Information

because of its value in exploiting and stealing their identities. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

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

9. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

10. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiffs and Class Members have suffered injuries and damages as a result of Defendant's conduct. These injuries include (i) misuse of their Private Information, (ii) actual identity theft and fraud, (iii) invasion of privacy; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (vi) anxiety, depression, and emotional harm; (vii) loss of benefit of the bargain; (viii) an increase in spam calls, texts, and/or emails; and (ix) the continued and

certainly increased risk to their Private Information, which remains unencrypted and vulnerable in Defendant's possession and subject to further unauthorized disclosure, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

12. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves, and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiffs

13. Plaintiff Sebastian Schug is an adult individual and a citizen and resident of Van Nuys, California, where he intends to remain.

14. Plaintiff Joseph DosReis is an adult individual and a citizen and resident of Jacksonville, Florida, where he intends to remain.

15. Plaintiff Phillip McLaughlin is an adult individual and a citizen and resident of Kissimmee, Florida, where he intends to remain.

16. Plaintiff Kimberly Thompson is an adult individual and a citizen and resident of Louisville, Kentucky, where she intends to remain.

17. Plaintiff Tyreese Banks is an adult individual and a citizen and resident of Wyoming, Michigan, where he intends to remain.

18. Plaintiff Maria Alvarez is an adult individual and a citizen and resident of New York, New York, where she intends to remain.

19. Plaintiff Suzzette Katzman is an adult individual and a citizen and resident of East Bend, North Carolina, where she intends to remain.

20. Plaintiff Lily Peace is an adult individual and a citizen and resident of Jamestown, North Dakota, where she intends to remain.

21. Plaintiff Duane Hopson is an adult individual and a citizen and resident of Columbus, Ohio, where he intends to remain.

22. Plaintiff Andy Lavor, parent and legal guardian of his daughter I.L., is an adult individual and a citizen and resident of Erie, Pennsylvania, where he intends to remain. Plaintiff Andy Lavor represents the interests of his daughter, I.L., a minor individual and citizen and resident of Erie, Pennsylvania, where she intends to remain.

23. Plaintiff Fortesa Bobo is an adult individual and a citizen and resident of Spartanburg, South Carolina, where she intends to remain.

24. Plaintiff Jalisa Bogan is an adult individual and a citizen and resident of Memphis, Tennessee, where she intends to remain.

25. Plaintiff Augusta Burkes is an adult individual and a citizen and resident of Clarksville, Tennessee, where she intends to remain.

26. Plaintiff Heather Robison is an adult individual and a citizen and resident of Fort Worth, Texas, where she intends to remain.

Defendant

27. Defendant is a Delaware corporation with its principal place of business located in Charlotte, North Carolina.

JURISDICTION AND VENUE

28. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is 161,676 and at least one member of the Class

(including multiple Plaintiffs) is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

29. This Court has general personal jurisdiction over Defendant because it is a North Carolina citizen with its principal place of business located in this state.

30. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant is subject to the Court's personal jurisdiction with respect to this action.

FACTUAL ALLEGATIONS

Defendant's Collection of Private Information

31. Defendant is multinational doughnut company and coffeehouse chain.

32. Plaintiffs and Class Members are Defendant's current and former employees, who provided their Private Information to Defendant as a condition and in exchange for their employment.

33. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

34. Upon information and belief, Defendant made promises and representations to its employees, including Plaintiffs and Class Members, that their Private Information would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

35. Indeed, Defendant's Privacy Policy posted on its website states, "We take administrative, technical and organizational measures to protect your information against

accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access."[1]

36. Plaintiffs' and Class Members' Private Information was provided 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.

37. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

38. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep individuals' Private Information safe and confidential.

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

40. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

41. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

[1] https://www.krispykreme.com/legal/privacy-policy (last visited Oct. 13, 2025).

42. 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 disclosure.

The Data Breach

43. On or about June 16, 2025, Defendant sent out notice ("Notice Letters") informing Plaintiffs and Class Members of the Data Breach.

44. The Notice of Data Security Incident posted on Defendant's website ("Website Notice") stated in relevant part as follows:

> On November 29, 2024, Krispy Kreme became aware of unauthorized activity on a portion of its information technology systems. Upon learning of the unauthorized activity, we immediately began taking steps to investigate, contain, and remediate the incident with the assistance of leading cybersecurity experts. On May 22, 2025, our investigation into the incident determined that certain personal information was affected. There is no evidence that the information has been misused, and we are not aware of any reports of identity theft or fraud as a direct result of this incident. This notification has not been delayed as the result of a law enforcement investigation.
>
> . . .
>
> Types of information that were subject to unauthorized access vary by individual but may include: name, Social Security number, date of birth, driver's license or state ID number, financial account information, financial account access information, credit or debit card information, credit or debit card information in combination with a security code, username and password to a financial account, passport number, digital signature, username and password, email address and password, biometric data, USCIS or Alien Registration Number, US military ID number, medical or health information, and health insurance information.

45. Omitted from the Notice Letters and Website Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to

ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

46. Defendant also failed to disclose that the notorious Play ransomware group perpetrated the Data Breach, let alone that Play had published Plaintiffs' and Class Members' stolen Private Information on its dark web leak site for any number of unknown and nefarious actors to take and further misuse.

47. Thus, Defendant's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

48. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

49. Hackers accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members; Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

50. Plaintiffs further believe that their Private Information, and that of Class Members, was and will be subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

51. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew the Risk of a Cyberattack.

52. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

53. Data thieves regularly target institutions and large employers like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

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

55. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

56. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

57. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

58. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially tens of thousands of individuals detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

59. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

60. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Private Information

61. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[3]

[2] 17 C.F.R. § 248.201 (2013).
[3] *Id.*

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

63. For example, Private Information can be sold at a price ranging from $40 to $200. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

64. Theft of PHI is also gravely serious: A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.

65. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.

66. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[4]

67. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive to restore coverage.[5] Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.

---

[4] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[5] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

68. Thus, the information compromised in this Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because the information compromised in this Data Breach—like Social Security numbers—is impossible to "close" and difficult, if not impossible, to change.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[6]

70. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

71. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches,

> in 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.[7]

Defendant Failed to Comply with FTC Guidelines.

72. The FTC has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has

---

[6] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[7] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

concluded a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an unfair practice in violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

77. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTC Act. Despite this, Defendant failed to comply with these obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Failed to Comply with HIPAA.

78. To the extent Defendant collects PHI as a sponsor of employee group health plans, Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

79. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

80. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

81. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

82. HIPAA requires "comply[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

83. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

84. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

85. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to

those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

86. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

87. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

88. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

89. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

90. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the

confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.

91. Defendant was at all times fully aware of its HIPAA obligations to protect Private Information yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

92. Experts studying cybersecurity routinely identify food chains like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

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

94. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical

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

95. Upon information and belief, Defendant failed to implement industry standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

96. Defendant failed to comply with these accepted standards, thereby causing the Data Breach to occur.

Defendant Breached Its Duty to Safeguard Plaintiffs and Class Members' Private Information.

97. In addition to its obligations under federal laws, Defendant owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

98. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Plaintiffs' and Class Members' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

99. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems, which contained unsecured and unencrypted Private Information.

100. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

Plaintiffs and Class Members Suffered Common Injuries & Damages.

101. 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 (a) misuse of Private Information; (b) actual identity theft and fraud; (c) materialized and imminent risk of identity theft and fraud; (d) invasion of privacy; (e) loss of time, loss of

productivity, and expenses incurred addressing identity theft and fraud; (f) loss of time, loss of productivity, and expenses incurred mitigating the materialized risk and imminent threat of identity theft risk; (g) the loss of benefit of the bargain; (h) diminished value of their Private Information; (i) invasion of privacy; and (j) the continued risk to their Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

The Data Breach Increases Victims' Risk of Identity Theft.

102. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

103. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

104. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

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

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

107. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[8]

108. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

109. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still

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

easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

110. 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 resource of time has been lost.

111. Plaintiffs and Class Members have spent, and will spend in the future, substantial time on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts, changing passwords and re-securing their own computer networks, and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

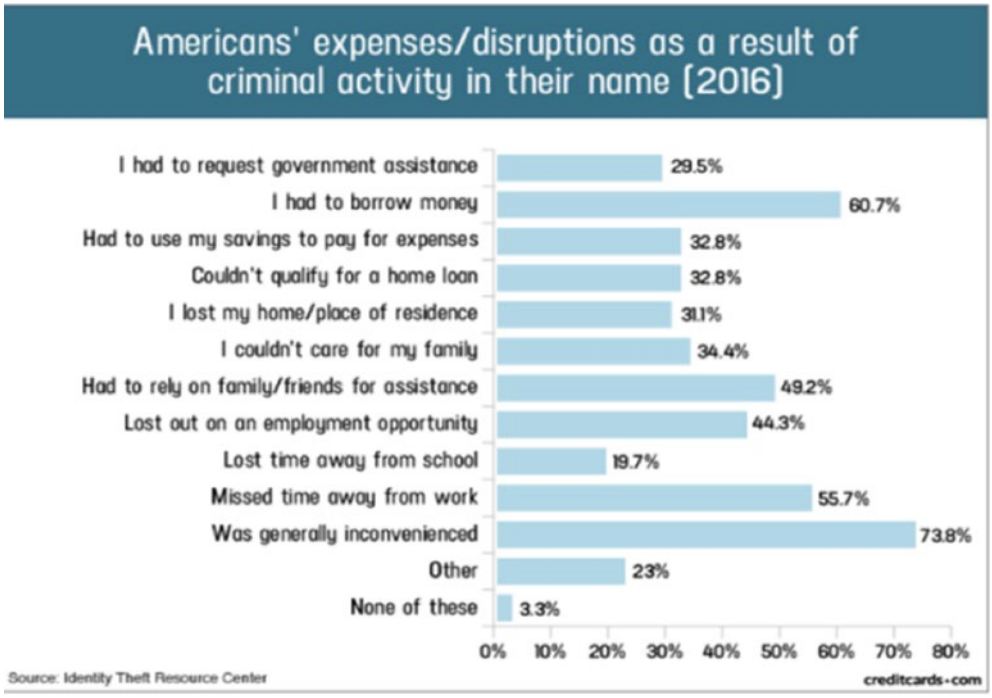
112. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

113. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended

[9] *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.

fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

114. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[10]



Diminished Value of Private Information

115. PII and PHI are valuable property rights. Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

116. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.

[10] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

117. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.

118. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.

119. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

120. 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 their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

121. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network, amounting to hundreds of thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

122. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Reasonable and Necessary Cost of Credit and Identity Theft Monitoring

123. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

124. Such fraud may go undetected for years; consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

125. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from the 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.

Plaintiffs' Experiences

Plaintiff Fortesa Bobo

126. Plaintiff Bobo is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

127. As a condition of obtaining employment, Plaintiff Bobo was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

128. Plaintiff Bobo greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Bobo diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

129. At the time of the Data Breach, Defendant retained Plaintiff Bobo's Private Information on its systems with inadequate data security, causing Plaintiff Bobo's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

130. Plaintiff Bobo received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised.

131. Plaintiff Bobo's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

132. Plaintiff Bobo's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Bobo's Private Information in the Data Breach, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

133. As a result of the Data Breach, Plaintiff Bobo has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, and contacting counsel regarding the Data Breach –valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

134. Plaintiff Bobo further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data

Breach, Plaintiff Bobo is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

135. The risk of identity theft is impending and has materialized, as Plaintiff Bobo's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

136. Plaintiff Bobo further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

137. Plaintiff Bobo has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information her, such as his or her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

138. The Data Breach has caused Plaintiff Bobo to suffer fear, anxiety, and stress, especially given that her Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft she now faces as a result.

Plaintiff Lily Peace

139. Plaintiff Peace is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

140. As a condition of obtaining employment, Plaintiff Peace was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

141. Plaintiff Peace greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Peace diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

142. At the time of the Data Breach, Defendant retained Plaintiff Peace's Private Information on its systems with inadequate data security, causing Plaintiff Peace's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

143. Plaintiff Peace received a Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised.

144. Plaintiff Peace's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

145. Plaintiff Peace's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Peace's Private Information in the Data Breach, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

146. As a result of the Data Breach, Plaintiff Peace has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, and contacting counsel regarding the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

147. Plaintiff Peace further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Peace is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. The risk of identity theft is impending and has materialized, as Plaintiff Peace's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

149. Plaintiff Peace further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

150. Plaintiff Peace has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information her, such as his or her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

151. The Data Breach has caused Plaintiff Peace to suffer fear, anxiety, and stress, especially given that her Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft she now faces as a result.

Plaintiff Jalisa Bogan

152. Plaintiff Bogan is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

153. As a condition of obtaining employment, Plaintiff Bogan was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

154. Plaintiff Bogan greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Bogan diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

155. At the time of the Data Breach, Defendant retained Plaintiff Bogan's Private Information on its systems with inadequate data security, causing Plaintiff Bogan's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

156. Plaintiff Bogan received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised.

157. Plaintiff Bogan's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

158. Plaintiff Bogan's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Bogan's Private Information in the Data Breach, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

159. Additionally, Plaintiff Bogan's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud against her: Following the Data Breach, unauthorized actors misused Plaintiff Bogan's Private Information for at least three

unauthorized and fraudulent transactions—one fraudulent charge of $700, one for $0, and one for an specified amount that stated the amount would be confirmed after processing. All three fraudulent transactions appeared on Plaintiff Bogan's credit history as delinquent/unpaid. Additionally, the fraudulent transactions had a negative impact on Plaintiff Bogan's credit, which may take Plaintiff Bogan years to restore.

160. As a result of the Data Breach, Plaintiff Bogan has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, and contacting counsel regarding the Data Breach. Plaintiff Bogan also spent considerable time investigating and disputing the fraudulent transactions and instances of identity theft using her Private Information. All the time Plaintiff Bogan was forced to expend due to the Data Breach is valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

161. Due to the Data Breach, Plaintiff Bogan has incurred out-of-pocket losses addressing her Private Information's disclosure and mitigating her now-heightened risk of identity theft and fraud, including credit monitoring and identity theft protection services at a cost of $69.00 per year, which she would not have incurred but for the Data Breach.

162. Plaintiff Bogan further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Bogan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

163. The risk of identity theft is impending and has materialized, as Plaintiff Bogan's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

164. Plaintiff Bogan further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

165. Plaintiff Bogan has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information her, such as his or her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

166. The Data Breach has caused Plaintiff Bogan to suffer fear, anxiety, and stress, especially given that her Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft she now faces as a result. Plaintiff Bogan is frightened for her physical safety given that any bad actor can now obtain and misuse her Private Information for further crimes against her due to the Data Breach.

Plaintiff Sebastian Schug

167. Plaintiff Schug is a former employee of Defendant and provided his Private Information to Defendant in exchange for employment.

168. As a condition of obtaining employment, Plaintiff Schug was required to supply Defendant with Private Information including his name, date of birth, and Social Security number.

169. Plaintiff Schug greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Schug diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

170. At the time of the Data Breach, Defendant retained Plaintiff Schug's Private Information on its systems with inadequate data security, causing Plaintiff Schug's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

171. Plaintiff Schug received Defendant's Notice Letter dated June 16, 2025, informing that his Private Information including name and Social Security number was compromised.

172. Plaintiff Schug's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

173. Plaintiff Schug's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Schug's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

174. As a result of the Data Breach, Plaintiff Schug has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring his accounts and changing passwords, and contacting counsel regarding the Data Breach —valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

175. Plaintiff Schug further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data

Breach, Plaintiff Schug is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

176. The risk of identity theft is impending and has materialized, as Plaintiff Schug's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

177. Plaintiff Schug further believes his Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

178. Plaintiff Schug has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information him, such as his phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

179. The Data Breach has caused Plaintiff Schug to suffer anxiety and stress because he expected Defendant to reasonably protect his Private Information, and especially given that his Private Information has now been published on the dark web, causing a continuing invasion of privacy and risk of identity theft.

Plaintiff Tyreese Banks

180. Plaintiff Banks is a former employee of Defendant and provided his Private Information to Defendant in exchange for employment.

181. As a condition of obtaining employment, Plaintiff Banks was required to supply Defendant with Private Information including his name, date of birth, and Social Security number.

182. Plaintiff Banks greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Banks diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

183. At the time of the Data Breach, Defendant retained Plaintiff Banks's Private Information on its systems with inadequate data security, causing Plaintiff Banks's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

184. Plaintiff Banks received Defendant's Notice Letter dated June 16, 2025, informing that his Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

185. Plaintiff Banks's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

186. Plaintiff Banks's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Banks's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

187. As a result of the Data Breach, Plaintiff Banks has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to approximately 20 hours to date researching and verifying the legitimacy of the Data Breach, monitoring his accounts, and changing passwords, and contacting counsel regarding the Data Breach—valuable time he

otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

188. Plaintiff Banks further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Banks is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

189. The risk of identity theft is impending and has materialized, as Plaintiff Banks's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

190. Plaintiff Banks further believes his Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

191. Plaintiff Banks has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information him, such as his or his phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

192. The Data Breach has caused Plaintiff Banks to suffer fear, anxiety, and stress about negative impacts to his finances and credit, especially given that his Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft he now faces as a result.

Plaintiff Maria Alvarez

193. Plaintiff Alvarez is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

194. As a condition of obtaining employment, Plaintiff Alvarez was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

195. Plaintiff Alvarez greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Alvarez diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

196. At the time of the Data Breach, Defendant retained Plaintiff Alvarez's Private Information on its systems with inadequate data security, causing Plaintiff Alvarez's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

197. Plaintiff Alvarez received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

198. Plaintiff Alvarez's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

199. Plaintiff Alvarez's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Alvarez's Private Information in the Data Breach, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

200. Additionally, subsequent to and due to the Data Breach, Plaintiff Alvarez has received multiple alerts from Capital One and American Express that her Private Information has been found published on the dark web, and notifications informing that her account passwords have been compromised.

201. In addition, as a result of the Data Breach, cybercriminals misused Plaintiff Alvarez's Private Information to make a frightening and extortionary phone call to Plaintiff Alvarez's mother, claiming that Plaintiff Alvarez had been kidnapped and demanding a ransom payment for her release. The caller referred to Plaintiff Alvarez's full name and address, as well as her mother's name and address. This was a direct consequence of Plaintiff Alvarez's Private Information being exposed in the Data Breach, and exemplifies the significant invasion of privacy and emotional distress Plaintiff Alvarez is suffering as a result.

202. As a result of the Data Breach, Plaintiff Alvarez has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to at least 10 hours to date researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, and contacting counsel regarding the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Additionally, Plaintiff Alvarez spent time placing a credit freeze on her accounts and removing it when she needs to use her credit, causing her additional inconvenience she would not have experienced but for the Data Breach. This time has been lost forever and cannot be recaptured.

203. Plaintiff Alvarez further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data

Breach, Plaintiff Alvarez is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

204. The risk of identity theft is impending and has materialized, as Plaintiff Alvarez's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

205. Plaintiff Alvarez further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

206. Plaintiff Alvarez has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about her, such as her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

207. The Data Breach has caused Plaintiff Alvarez to suffer fear, anxiety, and stress, especially given that cybercriminals are now misusing her Private Information to make extortionary calls to Plaintiff Alvarez's family, and due to her Private Information being published on the dark web and the resulting invasion of privacy and risk of identity theft she now faces.

Plaintiff Augusta Burkes

208. Plaintiff Burkes is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

209. As a condition of obtaining employment, Plaintiff Burkes was required to supply Defendant with Private Information including her name, date of birth, Social Security number, and financial account information.

210. Plaintiff Burkes greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Burkes diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

211. At the time of the Data Breach, Defendant retained Plaintiff Burkes's Private Information on its systems with inadequate data security, causing Plaintiff Burkes's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

212. Plaintiff Burkes received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name and Social Security number was compromised in the Data Breach.

213. Plaintiff Burkes's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

214. Plaintiff Burkes's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Burkes's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

215. Additionally, subsequent to and due to the Data Breach, Plaintiff Burkes received an alert from her credit monitoring service that her Private Information has been found published on the dark web.

216. As a result of the Data Breach, Plaintiff Burkes has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to at least 20 hours to date researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, and contacting counsel regarding the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

217. Due to the Data Breach, Plaintiff Burkes has incurred out-of-pocket losses addressing her Private Information's disclosure and mitigating her now-heightened risk of identity theft and fraud, including credit monitoring and identity theft protection services with IDX at a cost of $25.00 per month, which she would not have incurred but for the Data Breach.

218. Plaintiff Burkes further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Burkes is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

219. The risk of identity theft is impending and has materialized, as Plaintiff Burkes's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

220. Plaintiff Burkes further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

221. Plaintiff Burkes has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information her, such as his or her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

222. The Data Breach has caused Plaintiff Burkes to suffer fear, anxiety, and stress, especially given that her Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft she now faces as a result. Plaintiff Burkes is frightened for her physical safety given that any bad actor can now obtain and misuse her Private Information for further crimes against her due to the Data Breach.

Plaintiff Joseph DosReis

223. Plaintiff DosReis is a former employee of Defendant and provided his Private Information to Defendant in exchange for employment.

224. As a condition of obtaining employment, Plaintiff DosReis was required to supply Defendant with Private Information including his name, date of birth, and Social Security number.

225. Plaintiff DosReis greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff DosReis diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

226. At the time of the Data Breach, Defendant retained Plaintiff DosReis's Private Information on its systems with inadequate data security, causing Plaintiff DosReis's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

227. Plaintiff DosReis received Defendant's Notice Letter dated June 16, 2025, informing that his Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

228. Plaintiff DosReis's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

229. Plaintiff DosReis's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff DosReis's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

230. As a result of the Data Breach, Plaintiff DosReis has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring his accounts, and changing passwords, and contacting counsel regarding the Data Breach--valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

231. Plaintiff DosReis further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff DosReis is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

232. The risk of identity theft is impending and has materialized, as Plaintiff DosReis's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

233. Plaintiff DosReis further believes his Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

234. Plaintiff DosReis has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information him, such as his or his phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

235. The Data Breach has caused Plaintiff DosReis to suffer fear, anxiety, and stress about negative impacts to his finances and credit, especially given that his Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft he now faces as a result.

Plaintiff Andy Lavor, as parent and legal guardian of his daughter I.L.

236. Plaintiff Lavor's daughter I.L. is a current employee of Defendant and provided her Private Information to Defendant in exchange for employment.

237. As a condition of obtaining employment, I.L. was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

238. I.L. greatly values her privacy and is very careful about sharing her sensitive Private Information. I.L. diligently protects her Private Information and stores any documents containing

Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

239. At the time of the Data Breach, Defendant retained I.L.'s Private Information on its systems with inadequate data security, causing I.L.'s Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

240. I.L. received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised.

241. I.L.'s Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

242. I.L.'s Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted I.L.'s Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

243. I.L. anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, I.L. is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Given that I.L. is a minor, this continuing risk to her credit and identity is particularly harmful, as her credit are in danger of being destroyed before she even has a chance to build it.

244. The risk of identity theft is impending and has materialized, as I.L.'s and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

245. I.L. further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is

the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

246. I.L. has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information her, such as his or her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

247. The Data Breach has caused I.L. to suffer fear, anxiety, and stress, especially given that her Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft she now faces as a result. Additionally, I.L. has suffered a high degree of stress and anxiety because as a minor, she has yet to pull her credit so the damage from the Data Breach remains unknown. I.L. was planning to apply for a credit card and finance a car when she turns 18 in a few months, and now worries when that time comes, her credit will already be destroyed due to the Data Breach.

Plaintiff Heather Robison

248. Plaintiff Robison is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

249. As a condition of obtaining employment, Plaintiff Robison was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

250. Plaintiff Robison greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Robison diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

251. At the time of the Data Breach, Defendant retained Plaintiff Robison's Private Information on its systems with inadequate data security, causing Plaintiff Robison's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

252. Plaintiff Robison received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

253. Plaintiff Robison's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

254. Plaintiff Robison's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Robison's Private Information in the Data Breach, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

255. Additionally, Plaintiff Robison's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud against her: Following the Data Breach, unauthorized actors misused Plaintiff Robison's Private Information for at least two unauthorized and fraudulent transactions to her bank account. As a result, Plaintiff Robison had to cancel her debit card and obtain a new one.

256. Plaintiff Robison's Private Information compromised the Data Breach was also misused in connection with two unauthorized attempts to login to her email account, which is the same email account she used when employed with Defendant.

257. As a result of the Data Breach, Plaintiff Robison has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to at least 30 hours to date researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, contacting counsel regarding the Data Breach, contacting her bank about the fraudulent transactions to her account, and cancelling and ordering a new debit card—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

258. Plaintiff Robison further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Robison is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

259. The risk of identity theft is impending and has materialized, as Plaintiff Robison's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

260. Plaintiff Robison further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

261. Plaintiff Robison has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, mail, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about her, such as her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information. The amount of spam

communications Plaintiff Robison has received since and due to the Data Breach is extreme, typically 10–20 calls a day and 5–10 physical letters a week.

262. The severe increase in spam calls Plaintiff Robison receives each day due to the Data Breach has significantly and negatively impacted her life. The constant calls have hurt her ability to stay on top of work tasks because she cannot be sure if incoming calls are related to her job or just spam. Additionally, due to her phone being flooded with scams, Plaintiff Robison has missed important calls regarding her family, including one call about her son being injured, which Plaintiff Robison did not answer fearing it was just another bad actor spamming her.

263. The Data Breach has caused Plaintiff Robison to suffer fear, anxiety, and stress, especially given that her Private Information has published on the dark web and the resulting invasion of privacy and risk of identity theft she now faces, and the significant intrusion into her private and professional life due to the severe uptick in spam communications she has received.

Plaintiff Duane Hopson

264. Plaintiff Hopson is a former employee of Defendant and provided his Private Information to Defendant in exchange for employment.

265. As a condition of obtaining employment, Plaintiff Hopson was required to supply Defendant with Private Information including his name, date of birth, and Social Security number.

266. Plaintiff Hopson greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Hopson diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

267. At the time of the Data Breach, Defendant retained Plaintiff Hopson's Private Information on its systems with inadequate data security, causing Plaintiff Hopson's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

268. Plaintiff Hopson received Defendant's Notice Letter dated June 16, 2025, informing that his Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

269. Plaintiff Hopson's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

270. Plaintiff Hopson's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Hopson's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

271. Additionally, Plaintiff Hopson's Private Information compromised in the Data Breach has already been misused to commit extensive identity theft and fraud against him.

272. Following the Data Breach, unauthorized actors misused Plaintiff Hopson's Private Information to purchase an unauthorized and fraudulent subscription to DoorDash for $17.00 per month, paid using Plaintiff Hopson's account starting in or around January 2025. Because he also uses DoorDash, at first Plaintiff Hopson did not realize the subscription charges were fraudulent. However, after his accounts were shorter in funds than expected week after week, Plaintiff Hopson investigated, noticed the suspicious charges, and called DoorDash to inquire. He was then informed by DoorDash that the recurring charges were for a subscription, which Plaintiff Hopson had not purchased. While Plaintiff Hopson has since been communicating with his bank about the

fraudulent charges, he remains unreimbursed for these losses to date. As a result of this identity theft, Plaintiff Hopson was forced to cancel his debit card and obtain a new one. On multiple occasions, the unauthorized charges also caused Plaintiff Hopson's account to overdraft, resulting in him incurring out-of-pocket charges for overdraft fees. While Plaintiff Hopson was able to get some overdraft charges reversed, the majority—totalling approximately $370—have not been reimbursed.

273. Additionally, Plaintiff Hopson experienced actual identity theft due to the Data Breach in the form of multiple unauthorized charges to Plaintiff Hopson's Apple Card since approximately June 2025.

274. Plaintiff Hopson was again the victim of identity theft due to the Data Breach in or around July 2025, when an unauthorized actor used Plaintiff Hopson's compromised Private Information to apply for a loan with FastLoan.com in Plaintiff Hopson's name. A letter informing that the loan application was rejected was forwarded to Plaintiff Hopson's current address from his previous address, which was used for the loan application. Although the loan was not approved, Plaintiff Hopson's credit score dropped as a result.

275. Further, following and due to the Data Breach, Plaintiff Hopson received an alert that an unknown device was attempting to log on to Plaintiff Hopson's father's CashApp account (Plaintiff Hopson had power of attorney over his father before his recent passing).

276. Further, due to the Data Breach and his Private Information's compromise, Plaintiff Hopson is now unable to send or receive money using Venmo or Apple Pay due to both apps' stated inability to verify his identity, despite Plaintiff Hopson submitting additional supporting documentation.

277. Since and due to the Data Breach, Plaintiff Hopson also received an alert from Gmail that his Private Information was found posted on the dark web.

278. As a result of the Data Breach, Plaintiff Hopson has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to ***hundreds*** of hours to date researching and verifying the legitimacy of the Data Breach, monitoring his accounts, changing his account passwords, cancelling his debit card, contacting DoorDash about fraudulent transactions, disputing fraudulent transactions with his bank and credit card company, communicating with and submitting supporting documentation to Apple Pay and Venmo in attempts to re-verify his identity, investigating unauthorized loan applications in his name, cancelling his CashApp account, disputing overdraft charges, changing his phone number due to spam calls and texts, and contacting counsel regarding the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

279. Plaintiff Hopson further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Hopson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

280. The risk of identity theft is impending and has materialized, as Plaintiff Hopson's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

281. Plaintiff Hopson further believes his Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

282. Plaintiff Hopson has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information him, such as his or his phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information. Due to the drastic increase in spam Plaintiff Hopson received due to the Data Breach, he was forced to get a new phone number in August 2025.

283. The Data Breach has caused Plaintiff Hopson to suffer fear, anxiety, stress, and depression. The Data Breach and the resulting misuse of his Private Information and identity theft forced Plaintiff Hopson into a spiral. The multiple fraudulent charges Plaintiff Hopson experienced and significant efforts he was forced to expend in an attempt to resolve them caused Plaintiff Hopson significant anxiety and stress. Plaintiff Hopson also went into a depression due to the significant financial costs he incurred and the negative impact to his credit. Prior to the Data Breach, Plaintiff Hopson was doing his best to get ahead in life and optimistic about the progress he was making with his finances, but now all that progress has been reversed.

Plaintiff Kimberly Thompson

284. Plaintiff Thompson is a current employee of Defendant and provided her Private Information to Defendant in exchange for employment.

285. As a condition of obtaining employment, Plaintiff Thompson was required to supply Defendant with Private Information including her name, date of birth, Social Security number, and financial account information.

286. Plaintiff Thompson greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Thompson diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

287. At the time of the Data Breach, Defendant retained Plaintiff Thompson's Private Information on its systems with inadequate data security, causing Plaintiff Thompson's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

288. Plaintiff Thompson received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

289. Plaintiff Thompson's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

290. Plaintiff Thompson's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Thompson's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

291. Additionally, Plaintiff Thompson's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud against her: Following the Data Breach (in December 2024 and January 2025), an unknown actor made two unauthorized and fraudulent charges for DoorDash using Plaintiff Thompson's Fiserv account.

292. In May 2025, Plaintiff Thompson was again the victim of identity theft due to the Data Breach, when an unauthorized actor attempted a fraudulent charge to Plaintiff Thompson's Chime account.

293. In the summer of 2025, Plaintiff Thompson's Private Information compromised in the Data Breach was again misused by an unauthorized actor attempting to log in to Plaintiff Thompson's Google account—where Plaintiff's debit and credit card information is saved—from Las Vegas, Nevada.

294. Due to the Data Breach, Plaintiff Thompson experienced additional identity theft when an unauthorized actor charged $571 to Plaintiff Thompson's Discover card. Plaintiff Thompson learned of this fraud only after it appeared on her Equifax report as delinquent in September 2025. Plaintiff has been working to have this substantial fraudulent charged reversed by Discover, but remains unreimbursed for that loss to date.

295. In or around August 2025, Plaintiff Thompson was denied after applying for a personal loan at her credit union, which came as a surprise to her at that time because she believed her credit was strong. Now that Plaintiff Thompson is aware of the fraudulent $571 charge to her Discover account that was reported as delinquent, she believes that is the reason her loan application was not approved.

296. As a result of the Data Breach, Plaintiff Thompson has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring her accounts on a weekly or daily basis, changing passwords, investigating and communicating with financial institutions about fraudulent charges, contacting counsel regarding the Data Breach, dealing with spam calls and texts, and

cancelling and ordering a new debit card—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

297. Due to the Data Breach, Plaintiff Thompson has incurred out-of-pocket losses addressing her Private Information's disclosure and mitigating her now-heightened risk of identity theft and fraud and the actual identity theft she already experienced, including credit monitoring and identity theft protection services with Credit Karma at a cost of $7.00 per month, which she would not have incurred but for the Data Breach.

298. Plaintiff Thompson further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Thompson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

299. The risk of identity theft is impending and has materialized, as Plaintiff Thompson's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

300. Plaintiff Thompson further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

301. Plaintiff Thompson has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about her, such as her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information. In or around April

2025, Plaintiff Thompson received a spam call purporting to be from a cruise line representative, who referred to the last four digits of Plaintiff Thompson's Fiserv account number and requested her to provide the CVV code for that account's debit card. As a result, Plaintiff Thompson was forced to cancel her card and obtain a new one.

302. The Data Breach has caused Plaintiff Thompson to suffer fear, anxiety, and stress, especially given that her Private Information has published on the dark web and the resulting invasion of privacy and risk of identity theft she now faces, and the significant intrusion into her private and professional life due to the severe uptick in spam communications she has received.

Plaintiff Suzzette Katzman

303. Plaintiff Katzman is a former employee of Defendant and provided her Private Information to Defendant in exchange for employment.

304. As a condition of obtaining employment, Plaintiff Katzman was required to supply Defendant with Private Information including her name, date of birth, and Social Security number.

305. Plaintiff Katzman greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Katzman diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

306. At the time of the Data Breach, Defendant retained Plaintiff Katzman's Private Information on its systems with inadequate data security, causing Plaintiff Katzman's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

307. Plaintiff Katzman received Defendant's Notice Letter dated June 16, 2025, informing that her Private Information including name, date of birth, and Social Security number was compromised.

308. Plaintiff Katzman's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

309. Plaintiff Katzman's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff Katzman's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

310. Additionally, due to the Data Breach Plaintiff Katzman's Private Information was misused in connection with a suspicious letter she received from her bank thanking her for opening a new account, which Plaintiff Katzman had not opened.

311. As a result of the Data Breach, Plaintiff Katzman has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, monitoring her accounts and changing passwords, contacting her bank regarding the suspicious letter about a new account in her name, and contacting counsel regarding the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

312. Plaintiff Katzman further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data

Breach, Plaintiff Katzman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

313. The risk of identity theft is impending and has materialized, as Plaintiff Katzman's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

314. Plaintiff Katzman further believes her Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

315. Plaintiff Katzman has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, mail, and/or emails following the Data Breach, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information her, such as his or her phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

316. The Data Breach has caused Plaintiff Katzman to suffer fear, anxiety, and stress, especially given that her Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft she now faces as a result. As Plaintiff Katzman is not very tech-savvy, she has suffered anxiety imaging all the unknowable bad actors accessing her sensitive data on the dark web. This anxiety is so severe it often causes Plaintiff Katzman to wake up in the middle of the night with fear.

Plaintiff Phillip McLaughlin

317. Plaintiff McLaughlin is a former employee of Defendant and provided his Private Information to Defendant in exchange for employment.

318. As a condition of obtaining employment, Plaintiff McLaughlin was required to supply Defendant with Private Information including his name, date of birth, financial account information, and Social Security number.

319. Plaintiff McLaughlin greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff McLaughlin diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

320. At the time of the Data Breach, Defendant retained Plaintiff McLaughlin's Private Information on its systems with inadequate data security, causing Plaintiff McLaughlin's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

321. Plaintiff McLaughlin received Defendant's Notice Letter dated June 16, 2025, informing that his Private Information including name, date of birth, and Social Security number was compromised in the Data Breach.

322. Plaintiff McLaughlin's Private Information was compromised in the Data Breach and stolen by cybercriminals, who illegally accessed Defendant's network for the specific purpose of targeting the Private Information and using it to commit identity theft and fraud.

323. Plaintiff McLaughlin's Private Information compromised in the Data Breach has already been misused: Play cybercriminals targeted Plaintiff McLaughlin's Private Information, stole it from Defendant's systems, held it for ransom, and published the data on the Play dark web leak site when Defendant did not pay.

324. As a result of the Data Breach, Plaintiff McLaughlin has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying

the legitimacy of the Data Breach, monitoring his accounts, and changing passwords, and contacting counsel regarding the Data Breach--valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

325. Plaintiff McLaughlin further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff McLaughlin is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

326. The risk of identity theft is impending and has materialized, as Plaintiff McLaughlin's and Class Members' Private Information was targeted, stolen, and disseminated on the dark web.

327. Plaintiff McLaughlin further believes his Private Information, and that of Class Members, will continue to be sold and disseminated on the dark web for years due to the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and visit dark web pages like the Play leak site.

328. Plaintiff McLaughlin has additionally suffered actual injury in the form of experiencing a severe increase in spam calls, texts, and/or emails following the Data Breach, including phishing texts attempting to compromise his PII further, which, upon information and belief, was caused by the Data Breach, given that cybercriminals are able to easily use the information compromised in the Data Breach to find more information him, such as his or his phone number or email address, from publicly available sources, including websites that aggregate and associate PII with the owner of such information.

329. The Data Breach has caused Plaintiff McLaughlin to suffer fear, anxiety, and stress about negative impacts to his finances and credit, especially given that his Private Information has now been published on the dark web, and the continuing invasion of privacy and risk of identity theft he now faces as a result. This stress and anxiety due to the Data Breach has also strained Plaintiff McLaughlin's home and family life.

CLASS ALLEGATIONS

330. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring this action on behalf of themselves, and on behalf of all members of the proposed nationwide class defined as follows:

> All individuals residing in the United States whose Private Information may have been compromised in the Data Breach ("Class").

331. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

332. Plaintiffs reserve the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

333. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

334. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believe the proposed Class includes at least tens of thousands of individuals who have been damaged by Defendant's conduct as alleged herein. According to the Office of the Main Attorney General, the Class is comprised 161,676 Class Members.

335. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include the following, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTC Act;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII 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 owed duties to Class Members to safeguard their PII;

h. Whether Defendant breached their duties to Class Members to safeguard their PII;

i. Whether hackers obtained Class Members' PII via the Data Breach;

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

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

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

m. What damages Plaintiffs and Class Members suffered from Defendant's conduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with its employees, including Plaintiffs and Class Members;

p. Whether Defendant were unjustly enriched;

q. Whether Plaintiffs and Class Members are entitled to damages;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

336. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves, and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

337. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

338. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The

common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

339. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

340. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or emails of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

341. Plaintiffs incorporate paragraphs 1 through 340, as if fully set forth herein.

342. Defendant's employees, including Plaintiffs and Class Members, provided their non-public Private Information to Defendant as a condition of obtaining employment with Defendant.

343. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

344. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

345. Defendant had duties to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

346. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the health care and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

347. 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 their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

348. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

349. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

350. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Allowing unauthorized access to Class Members' Private Information;

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

e. Failing to remove Plaintiffs' and Class Members' Private Information it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

351. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

352. Defendant's violation of federal statutes also constitutes negligence *per se*. Specifically, as described herein, Defendant has violated the FTC Act and HIPAA.

353. Plaintiffs and Class Members were within the class of persons the FTC Act and HIPPA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

354. Defendant has admitted that the Private Information of Plaintiffs and Class Members were wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

355. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

356. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

357. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (i) misuse of their Private Information, (ii) actual identity theft and fraud, (iii) invasion of privacy;

(iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (vi) anxiety, depression, and emotional harm; (vii) loss of benefit of the bargain; (viii) an increase in spam calls, texts, and/or emails; and (ix) the continued risk to their Private Information, which remains unencrypted and vulnerable in Defendant's possession and subject to further unauthorized disclosure, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

358. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

359. Plaintiffs incorporate paragraphs 1 through 340, as if fully set forth herein.

360. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining employment with Defendant.

361. Defendant solicited, offered, and invited Class Members to provide their Private Information in order to obtain employment at Defendant's. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

362. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing employment to Plaintiffs and Class Members.

363. Plaintiffs and Class Members entrusted their Private Information to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

364. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

365. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

366. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

367. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

368. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

369. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

370. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

371. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

372. North Carolina law provides that every contract includes good faith and fair dealing between the parties involved.

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

374. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their Private Information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that Private Information was compromised as a result of the Data Breach

375. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

376. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to (i) misuse of their Private Information, (ii) actual identity theft and fraud, (iii) invasion of privacy; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (vi) anxiety, depression, and emotional harm; (vii) loss of benefit of the bargain; (viii) an increase in spam calls, texts, and/or emails; and (ix) the continued risk to their Private Information, which remains unencrypted and vulnerable in Defendant's possession and subject to further unauthorized disclosure, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

377. Plaintiffs and Class Members are therefore entitled to compensatory, consequential, and nominal damages for Defendant's breach of implied contracts.

COUNT III

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

378. Plaintiffs incorporate paragraphs 1 through 340, as if fully set forth herein.

379. Plaintiffs and Class Members conferred a monetary benefit on Defendant; specifically, they provided their Private Information to Defendant to obtain employment.

380. The monies Defendant was paid in its ordinary course of business included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

381. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to

it. Defendant profited from Plaintiffs retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

382. Defendant enriched itself by hoarding the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheap, ineffective security measures and diverting those funds to its own personal use. 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 security and the safety of their Private Information.

383. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members, and as a result, Defendant was overpaid.

384. Under principles of equity and good conscience, Defendant should not be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

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

386. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (i) misuse of their Private Information, (ii) actual identity theft and fraud, (iii) invasion of privacy; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (vi) anxiety, depression, and emotional harm; (vii) loss of benefit of the bargain; (viii) an increase in spam calls, texts, and/or emails; and (ix) the continued risk to their Private Information, which remains unencrypted and vulnerable in

Defendant's possession and subject to further unauthorized disclosure, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

387. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and on behalf of the putative Class, pray for judgment against Defendant and the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. Injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order as follows:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all

applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

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

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to

segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. Actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. Attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: October 17, 2025

Respectfully submitted,

/s/ *Jeff Ostrow*
Jeff Ostrow (Pro Hac Vice)

KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-3200
ostrow@kolawyers.com

Scott Edward Cole, Esq.*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Tel: (510) 891-9800
sec@colevannote.com

Mariya Weekes*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
333 SE 2nd Avenue, Suite 2000
Miami, FL 33131
Tel: (866) 252-0878
mweekes@milberg.com

Interim Class Counsel

David M. Wilkerson
WILKERSON JUSTUS PLLC
P.O. Box 54
Asheville, NC 28804
Tel: (828) 316-6902
dwilkerson@wilkersonjustus.com

Interim Local Counsel

**pro hac vice* forthcoming