UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE CHRISTIE'S DATA BREACH LITIGATION, *This Document Relates To:* *All Member Cases*	Case No. 1:24-CV-4221 (JMF) CLASS ACTION DEMAND FOR JURY TRIAL

CONSOLIDATED CLASS ACTION COMPLAINT

Efstathios Maroulis, William Colley, Russell DeJulio, Alice Bruce, and Ildar Gaifullin (collectively, "Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Defendant Christie's Inc., ("Christie's" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a "world-leading art and luxury business" which is widely known for its "auctions [that] span more than 80 art and luxury categories, at price points ranging from $500 to over $100 million."[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former clients and customers, including full names, dates

[1] *About Christie's*, CHRISTIE'S, https://www.christies.com/en/about/overview (last visited June 14, 2024).

of birth, addresses, birthplaces, sex, nationality, document numbers, passport numbers, full Machine Readable Zone ("MRZ") numbers (the machine-readable code at the bottom of the identity page at the beginning of a passport, IDs, and visas), issuing authority, issue dates, expiration dates, and Driver's License Numbers (collectively, the "Private Information"). But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the Data Breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former clients' and customers' Private Information.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Private Information. In short, Defendant's failures placed the Class's Private Information in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs, as victims of the Christie's Data Breach, now bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this Data Breach, Christie's current and former clients' and customers' Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Efstathios Maroulis, is a natural person and citizen of Texas. He resides in Dallas, Texas where he intends to remain.

9. Plaintiff, William Colley, is a natural person and citizen of Alabama. He resides in DeKalb County, Alabama where he intends to remain.

10. Plaintiff, Russell DeJulio, is a natural person and citizen of Pennsylvania. He resides in Pittsburgh, Pennsylvania where he intends to remain.

11. Plaintiff, Alice Bruce, is a natural person and citizen of Florida. She resides in Lakeland, Florida where she intends to remain.

12. Plaintiff, Ildar Gaifullin, is a natural person and citizen of New York. He resides in Brooklyn, New York where he intends to remain.

13. Defendant, Christie's Inc., is a corporation incorporated in New York and with its principal place of business at 20 Rockefeller Plaza, New York, New York 10020.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. And there are over 100 putative Class Members.

15. This Court has personal jurisdiction over Defendant because it is headquartered in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

16. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiffs and the Class

17. Defendant is a "world-leading art and luxury business" which is widely known for its "auctions [that] span more than 80 art and luxury categories, at price points ranging from $500 to over $100 million."[2]

18. As part of its business, Defendant receives and maintains the PII of thousands of its current and former clients and customers.

19. In collecting and maintaining Plaintiffs' and Class Members' Private Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information.

20. Under state and federal law, businesses like Defendant have duties to protect its current and former clients' and customers' PII and to notify them about breaches.

21. Defendant recognizes these duties, declaring in its "Privacy Notice" that:

a. "This privacy notice applies to Christie's globally and explains the type of information that we process, why we are processing it and how that processing may affect you."[3]

[2] *About Christie's*, CHRISTIE'S, https://www.christies.com/en/about/overview (last visited August 19, 2024).
[3] *Privacy Notice*, CHRISTIE'S, https://www.christies.com/en/privacy-centre/privacy-notice/overview (last visited August 19, 2024).

b. "The information you provide to us will not be transmitted to other websites[.]"[4]

c. "We understand that your personal information is important and we are committed to treating it with the utmost care and security."[5]

d. "We have multiple layers of security technologies and controls in our environment which safeguard your data, while at rest or in transit, from unauthorised access or disclosure."[6]

e. "In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality."[7]

f. "In addition, our colleagues receive data protection training and we have in place detailed security and data protection policies which colleagues are required to follow when handling personal information."[8]

g. "In an ever-altering threat landscape, we are constantly assessing our security defences [sic] to ensure your data continues to stay protected."[9]

h. "We have put in place procedures to deal with any suspected personal data breach[.]"[10]

---

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

i. "We do not transfer your personal data to organisations who wish to use it for their own . . . purposes."[11]

j. "Your personal data will only be shared with organisations providing services to us or who need the information to enable us to provide you with services[.]"[12]

Defendant's Data Breach

22. On May 8, 2024, Defendant was hacked by cybercriminals in the Data Breach.[13]

23. Perhaps most troubling is that Defendant already admitted that cybercriminals successfully "copied" (i.e., exfiltrated) the Private Information from its data systems.[14]

24. Because of Defendant's Data Breach, it is currently known that ***highly sensitive*** PII was accessed and exfiltrated from Defendant's systems, including but not limited to, full names, passport information, driver's license information, and state and government-issued ID information.[15]

25. Notably, in an email to Plaintiffs and Class Members, Defendant admitted the following:

---

[11] *Id*.
[12] *Id*.
[13] *Data Breach Notification*, MAINE ATTY GEN, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7d04d0f1-25d1-45b1-b1d0-87ba72a4d343.shtml (last visited August 19, 2024).
[14] *Id*.
[15] *Data Breach Reports*, TEXAS ATTY GEN, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited August 19, 2024); *Data Breach Notice*, WASHINGTON ATTY GEN, https://www.atg.wa.gov/christie-s-inc (last visited Aug. 13, 2024).

a. "[D]uring the period of unauthorized access, the third party ***downloaded*** . . . client data from Christie's internal client verification system."

b. "The impacted personal data was data shown on the photographic identification that you provided to Christie's in the course of our routine client verification procedures."

c. "For Passports: the impacted data was the information shown on the ID page, including full name, gender, passport number, expiry date, date of birth, birth place, and MRZ (the machine-readable code at the bottom of the identity page at the beginning of a passport)."

d. "For other forms of ID (such as driving licenses and National Identity cards): the impacted data was the data shown on the front of the document, for example, full name, date of birth, country, and document number."

26. In total, Defendant's Data Breach impacted at least 45,798 persons—via the exposure and exfiltration of their Private Information—in the Data Breach.[16] Upon information and belief, these 45,798 persons include Defendant's current and former clients and customers.

27. However, third-party reports indicate that the true scope of the Data Breach includes approximately 500,000 of Defendant's current and former clients and customers.[17] Thus, upon information and belief, the size of the Class far exceeds 45,798 individuals.

---

[16] *Data Breach Notification*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/7d04d0f1-25d1-45b1-b1d0-87ba72a4d343.shtml (last visited August 18, 2024).

[17] *See e.g.,* Zachary Small, *After Hack, Christie's Gives Details of Compromised Client Data*, N.Y. TIMES (May 30, 2024) https://www.nytimes.com/2024/05/30/arts/design/christies-hack-client-data.html; Alicia Hope, *Christie's Auction House Confirms Data Breach after*

28. And when Defendant did finally notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "remain vigilant against incidents of identity theft and fraud by engaging in the following best practices;"

b. "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity;"

c. "contact [the FTC] for information on how to prevent or avoid identity theft[.]"[18]

29. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

30. Since the breach, Defendant has declared that it "continue[s] to evaluate technical and organizational measures to avoid the reoccurrence of a similar incident."[19]

31. However, Plaintiffs and Class Members remain at risk for another data breach until Defendant actually installs the technical and organizational measures necessary to prevent another data breach.

32. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

Ransomware Group Threatens to Leak Stolen Info, CPO MAGAZINE (June 4, 2024) https://www.cpomagazine.com/cyber-security/christies-auction-house-confirms-data-breach-after-ransomware-group-threatens-to-leak-stolen-info/.

[18] *Id.*

[19] *Id.*

33. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class Members for the injuries that Defendant inflicted upon them.

34. Because of Defendant's Data Breach, the sensitive Private Information of Plaintiffs and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Defendant's History of Negligent Data Security

35. Stunningly, this Data Breach is only part and parcel of Defendant's ***pattern*** of negligent data security. After all, in 2016, Defendant suffered another data breach which compromised the following types of PII:

a. names;

b. personal addresses;

c. business addresses;

d. personal phone numbers;

e. business phone numbers;

f. credit card numbers;

g. debit card numbers;

h. dates of birth; and

i. government-issued identification numbers.[20]

[20] *Legal Notice of Information Security Incident*, NEW HAMPSHIRE ATTY GEN (March 24, 2017) https://www.doj.nh.gov/consumer/security-breaches/documents/christies-20170324.pdf.

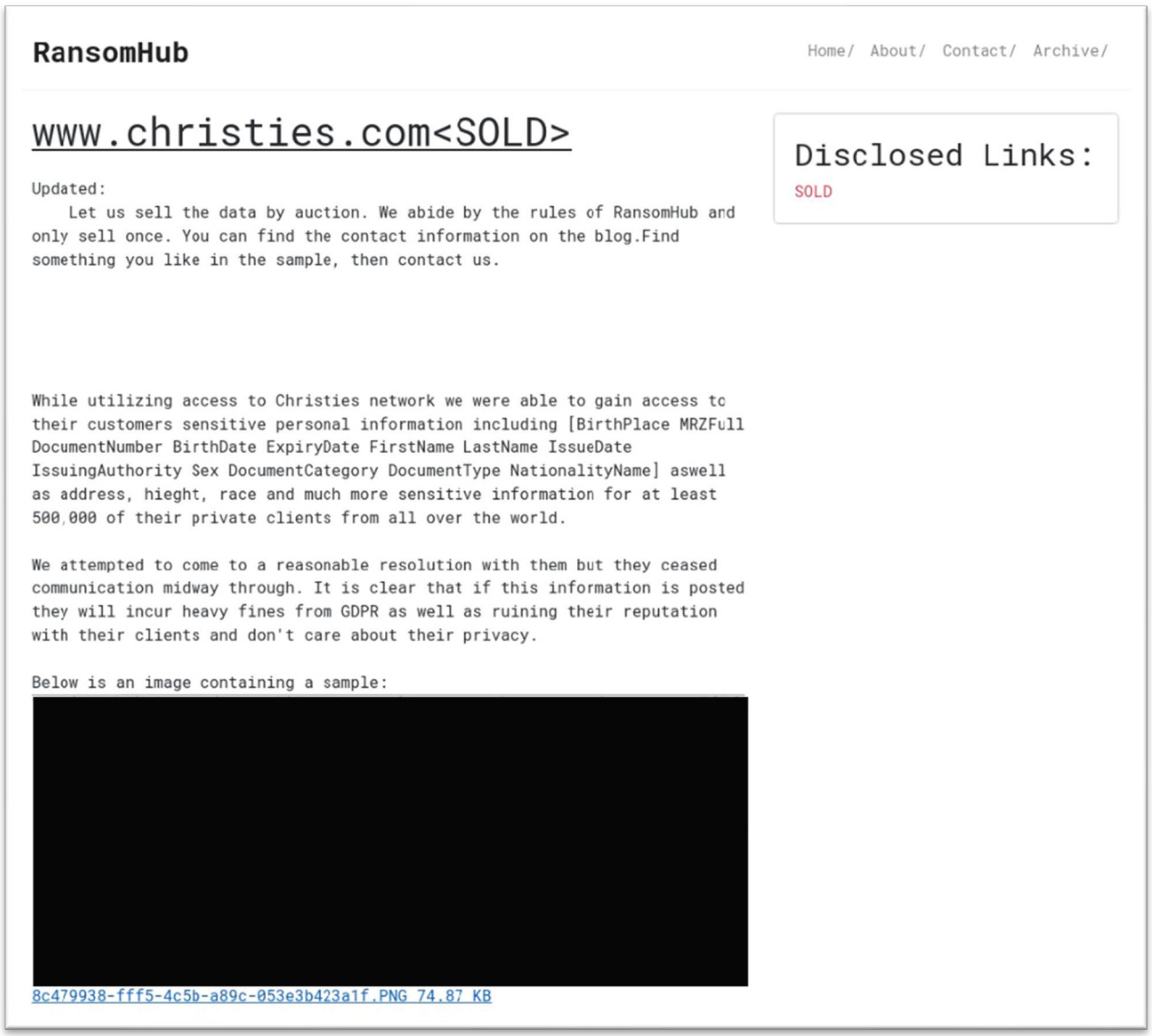
RansomHub & the Dark Web

36. The cybercriminals that obtained Plaintiffs' and Class Members' Private Information appear to be the notorious cybercriminal group "RansomHub."[21]

37. Notably, on its Dark Web webpage, RansomHub revealed that: "While utilizing access to Christies network we were able to gain access to their customers sensitive personal information including [BirthPlace MRZFull DocumentNumber BirthDate ExpiryDate FirstName LastName IssueDate IssuingAuthority Sex DocumentCategory DocumentType NationalityName] aswell as address, height, race and much more sensitive information for at least 500,000 of their private clients from all over the world [*sic*]."[22]

38. Furthermore, on June 4, 2024, RansomHub revealed on its Dark Web webpage that it had already ***published and sold*** the stolen Private Information.[23] Below is a screenshot of RansomHub's Dark Web webpage (with redactions to preserve victims' privacy).[24]

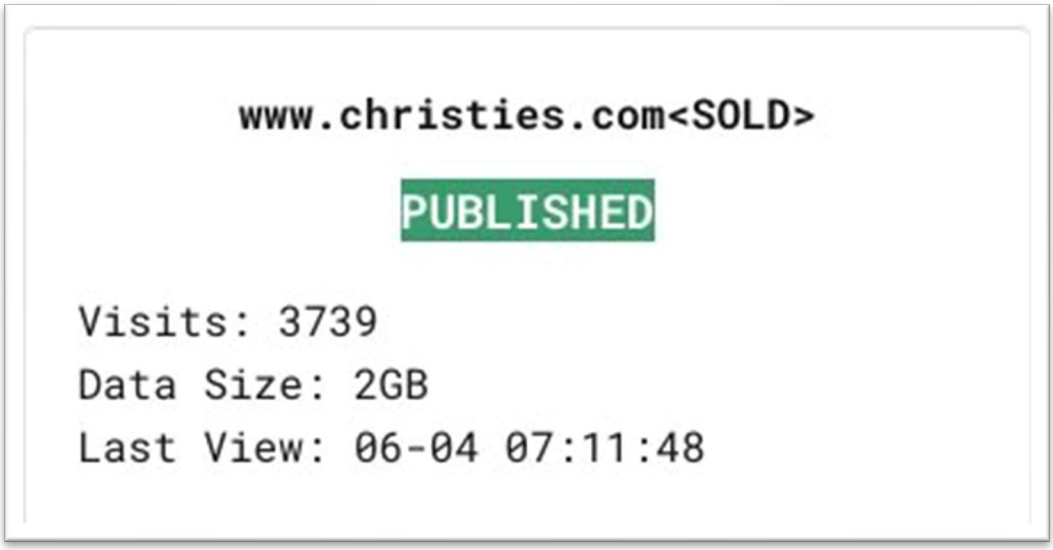
[21] Zachary Small, *Ransomware Group Claims Responsibility for Christie's Hack*, N.Y. TIMES (May 27, 2024) https://www.nytimes.com/2024/05/27/arts/design/hackers-claim-christies-attack.html.
[22] *RansomHub*, RANSOMLOOK (June 4, 2024) https://www.ransomlook.io/group/ransomhub.
[23] *Id*. https://www.idenfy.com/blog/machine-readable-zone/.
[24] *Id*.



39. Notably, the stolen Private Information seemingly consists of "2GB" (i.e., gigabytes) worth of data.[25]

40. To make matters worse, as of June 4, 2024, the published Private Information appears to have already been ***viewed*** by 3,739 "visit[or]s" to RansomHub's Dark Web webpage.[26] This, in and of itself, is a substantial violation of Plaintiffs' and Class Members' privacy.

[25] Dominic Alvieri (@AlvieriD), TWITTER (June 4, 2024) https://x.com/AlvieriD/status/1797890640677867964.
[26] *Id*.



41. Furthermore, third-party reports confirmed that "RansomHub held its own auction and sold the stolen data to an anonymous third party for an undisclosed sum."[27]

42. Unfortunately for Plaintiffs and the Class, RansomHub is notorious for following through on its threats and publishing and/or selling PII on the Dark Web.

43. Indeed, in April 2024, RansomHub sold PII on the Dark Web.[28] The PII in question was stolen from the healthcare system "Change Healthcare" and included medical records, dental records, payment claims, insurance details, and personal information like Social Security numbers and email addresses.[29]

44. Thus, on information and belief, Plaintiffs' and the Class's stolen Private Information has already been published—or will be published imminently—and/or sold by RansomHub on the Dark Web.

---

[27] Jonathan Reed, *Why the Christie's auction house hack is different*, SECURITY INTELLIGENCE (June 11, 2024) https://securityintelligence.com/news/why-christies-auction-house-hack-is-different/.
[28] Eric Geller, *Change Healthcare's New Ransomware Nightmare Goes From Bad to Worse*, WIRED (April 16, 2024, 3:09 PM) https://www.wired.com/story/change-healthcare-ransomhub-data-sale/.
[29] *Id*.

Plaintiff Maroulis' Experiences and Injuries

45. Plaintiff Maroulis is a former client of Defendant.

46. Thus, Defendant obtained and maintained Plaintiff's Private Information. As a result, Plaintiff's Private Information was exposed and exfiltrated by cybercriminals during Defendant's Data Breach.

47. As a condition of receiving products and/or services, Plaintiff provided Defendant with his Private Information. Defendant used that Private Information to facilitate its provision of products and/or services and to collect payment.

48. Plaintiff Maroulis provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

49. Plaintiff Maroulis is very careful about sharing his sensitive PII. Plaintiff Maroulis takes proactive steps to ensure that his PII is kept safe and secure and would never knowingly transmit unencrypted sensitive PII over the internet. Thus, Plaintiff would not have entrusted his Private Information to Defendant if Defendant was transparent about its negligent data security practices.

50. Plaintiff Maroulis reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

51. Plaintiff Maroulis received a Notice of Data Breach dated May 30, 2024.

52. Thus, on information and belief, Plaintiff Maroulis' Private Information has already been published—or will be published imminently—and/or sold by cybercriminals on the Dark Web.

53. Plaintiff Maroulis has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Maroulis to take those steps in its breach notice. This loss of time is significant and deprived Plaintiff Maroulis of the opportunity to dedicate this time to recreation or to earn money through work.

54. And in the aftermath of the Data Breach, Plaintiff Maroulis has suffered from a spike in spam and scam emails, text messages and phone calls. This misuse of PII is traceable to Defendant's Data Breach because cybercriminals routinely obtain information (e.g., phone numbers and email addresses) which can be found online and then target data breach victims with scam calls and messages (i.e., phishing) to elicit more sensitive information—which cybercriminals then combine with the Private Information exposed in a data breach to commit substantial identity theft and fraud.

55. Plaintiff Maroulis fears for his personal financial security and worries about what information was exposed in the Data Breach. Because of Defendant's Data Breach, Plaintiff Maroulis has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Maroulis' injuries are precisely the type of injuries that the law contemplates and addresses.

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

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

58. Plaintiff Maroulis has suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft that will continue for his lifetime—all because Defendant's Data Breach placed Plaintiff Maroulis' Private Information right in the hands of criminals.

59. Because of the Data Breach, Plaintiff Maroulis anticipates spending considerable amounts of time and money to try and mitigate his injuries.

60. Furthermore, Defendant's poor data security practices deprived Plaintiff Maroulis of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, Plaintiff Maroulis reasonably expected that Defendant would use reasonable data security to protect his Private Information (which Defendant required that Plaintiff Maroulis disclose). Thus, when Defendant failed to provide reasonable data security, Plaintiff Maroulis did not receive the full value of their bargain. After all, Plaintiff Maroulis would have paid less for Defendant's products and/or services if Defendant was forthcoming about the inadequacy of its data security practices.

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

Plaintiff Colley's Experiences and Injuries

62. Plaintiff Colley is a customer of Defendant.

63. Thus, Defendant obtained and maintained Plaintiff Colley's Private Information. As a result, Plaintiff Colley's Private Information was exposed and exfiltrated by cybercriminals during Defendant's Data Breach.

64. As a condition of receiving products and/or services, Plaintiff Colley provided Defendant with his Private Information. Defendant used that Private Information to facilitate its provision of products and/or services and to collect payment.

65. Plaintiff Colley provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Colley's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

66. Plaintiff Colley is very careful about sharing his sensitive PII. Plaintiff Colley takes proactive steps to ensure that his PII is kept safe and secure and would never knowingly transmit unencrypted sensitive PII over the internet. Thus, Plaintiff Colley would not have entrusted his Private Information to Defendant if Defendant was transparent about its negligent data security practices.

67. Plaintiff Colley reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

68. Plaintiff Colley received a Notice of Data Breach in or around May 30, 2024, and on June 7, 2024.

69. Thus, on information and belief, Plaintiff Colley's Private Information has already been published—or will be published imminently—and/or sold by cybercriminals on the Dark Web.

70. Plaintiff Colley has ***already*** suffered from the misuse of his Private Information when cybercriminals attempted to hack into his cell phone account after the Data Breach. This fraudulent activity is traceable to Defendant's Data Breach—which, upon information and belief, began earlier than Defendant has thus far determined and/or revealed.

71. Additionally, in the aftermath of the Data Breach, Plaintiff Colley has suffered from a spike in spam and scam emails and phone calls which appear to be targeted phishing attempts. This misuse of PII is traceable to Defendant's Data Breach because cybercriminals routinely obtain information (e.g., phone numbers and email addresses) which can be found online and then target data breach victims with scam calls and messages (i.e., phishing) to elicit more sensitive information—which cybercriminals then combine with the PII exposed in a data breach to commit substantial identity theft and fraud.

72. Plaintiff Colley has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Colley to take those steps in its breach notice. This loss of time is significant and deprived Plaintiff Colley of the opportunity to dedicate this time to recreation or to earn money through work.

73. Plaintiff Colley fears for his personal financial security and worries about what information was exposed in the Data Breach. Because of Defendant's Data Breach, Plaintiff Colley has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Colley's injuries are precisely the type of injuries that the law contemplates and addresses.

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

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

76. Plaintiff Colley suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft that will continue for his lifetime—all because Defendant's Data Breach placed Plaintiff Colley's Private Information right in the hands of criminals.

77. Because of the Data Breach, Plaintiff Colley anticipates spending considerable amounts of time and money to try and mitigate his injuries.

78. Furthermore, Defendant's poor data security practices deprived Plaintiff Colley of the benefit of his bargain. When agreeing to pay Defendant for products and/or services, Plaintiff Colley reasonably expected that Defendant would use reasonable data security to protect his Private Information (which Defendant required that Plaintiff Colley disclose). Thus, when Defendant failed to provide reasonable data security, Plaintiff Colley did not receive the full value of their bargain. After all, Plaintiff Colley would have paid less for Defendant's products and/or services if Defendant was forthcoming about the inadequacy of its data security practices.

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

Plaintiff DeJulio's Experiences and Injuries

80. Plaintiff DeJulio is a former client of Defendant.

81. Thus, Defendant obtained and maintained Plaintiff DeJulio's Private Information. As a result, Plaintiff DeJulio's Private Information was exposed and exfiltrated by cybercriminals during Defendant's Data Breach.

82. As a condition of receiving products and/or services, Plaintiff DeJulio provided Defendant with his Private Information. Defendant used that Private Information to facilitate its provision of products and/or services and to collect payment.

83. Plaintiff DeJulio provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff DeJulio's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

84. Plaintiff DeJulio is very careful about sharing his sensitive PII. Plaintiff DeJulio takes proactive steps to ensure that his PII is kept safe and secure and would never knowingly transmit unencrypted sensitive PII over the internet. Thus, Plaintiff DeJulio would not have entrusted his Private Information to Defendant if Defendant was transparent about its negligent data security practices.

85. Plaintiff DeJulio reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

86. Plaintiff DeJulio received a Notice of Data Breach dated June 7, 2024.

87. Plaintiff DeJulio has ***already*** suffered from the misuse of his compromised Private Information. After the Data Breach, he was notified that his name, driver's license number, phone number, emails, and passwords—were found published on the Dark Web.

88. After receiving this notification, Plaintiff DeJulio spent approximately 4 to 5 hours taking the following protective measures:

a. changing the passwords for all of his online accounts;

b. signing up for credit monitoring; and

c. calling his retirement account manager Vanguard, to warn them about the Data Breach and the compromise of his Private Information.

89. Plaintiff DeJulio has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff DeJulio to take those steps in its breach notice. This loss of time is significant and deprived Plaintiff DeJulio of the opportunity to dedicate this time to recreation or to earn money through work.

90. And in the aftermath of the Data Breach, Plaintiff DeJulio has suffered from a spike in spam and scam emails and phone calls which appear to be targeted phishing attempts. This misuse of PII is traceable to Defendant's Data Breach because cybercriminals routinely obtain information (e.g., phone numbers and email addresses) which can be found online and then target data breach victims with scam calls and messages (i.e., phishing) to elicit more sensitive information—which cybercriminals then combine with the PII exposed in a data breach to commit substantial identity theft and fraud.

91. Plaintiff DeJulio fears for his personal financial security and worries about what information was exposed in the Data Breach. Because of Defendant's Data Breach, Plaintiff DeJulio has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather,

Plaintiff DeJulio's injuries are precisely the type of injuries that the law contemplates and addresses.

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

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

94. Plaintiff DeJulio suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft that will continue for his lifetime—all because Defendant's Data Breach placed Plaintiff DeJulio's Private Information right in the hands of criminals.

95. Because of the Data Breach, Plaintiff DeJulio anticipates spending considerable amounts of time and money to try and mitigate his injuries.

96. Furthermore, Defendant's poor data security practices deprived Plaintiff DeJulio of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, Plaintiff DeJulio reasonably expected that Defendant would use reasonable data security to protect his Private Information (which Defendant required that Plaintiff DeJulio disclose). Thus, when Defendant failed to provide reasonable data security, Plaintiff DeJulio did not receive the full value of their bargain. After all, Plaintiff DeJulio would have paid less for Defendant's products and/or services if Defendant was forthcoming about the inadequacy of its data security practices.

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

Plaintiff Bruce's Experiences and Injuries

98. Plaintiff Bruce is a former client of Defendant.

99. Thus, Defendant obtained and maintained Plaintiff Bruce's Private Information. As a result, Plaintiff Bruce's Private Information was exposed and exfiltrated by cybercriminals during Defendant's Data Breach.

100. As a condition of receiving products and/or services, Plaintiff Bruce provided Defendant with her Private Information. Defendant used that Private Information to facilitate its provision of products and/or services and to collect payment.

101. Plaintiff Bruce provided her Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Bruce's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

102. Plaintiff Bruce is very careful about sharing her sensitive PII. Plaintiff Bruce takes proactive steps to ensure that her PII is kept safe and secure and would never knowingly transmit unencrypted sensitive PII over the internet. Thus, Plaintiff Bruce would not have entrusted her Private Information to Defendant if Defendant was transparent about its negligent data security practices.

103. Plaintiff Bruce reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

104. Plaintiff Bruce received a Notice of Data Breach dated June 7, 2024.

105. Thus, on information and belief, Plaintiff Bruce's Private Information has already been published—or will be published imminently—and/or sold by cybercriminals on the Dark Web.

106. Plaintiff Bruce has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff Bruce to take those steps in its breach notice. This loss of time is significant and deprived Plaintiff Bruce of the opportunity to dedicate this time to recreation or to earn money through work.

107. And in the aftermath of the Data Breach, Plaintiff Bruce has suffered from a spike in spam and scam emails, text messages and phone calls. This misuse of PII is traceable to Defendant's Data Breach because cybercriminals routinely obtain information (e.g., phone numbers and email addresses) which can be found online and then target data breach victims with scam calls and messages (i.e., phishing) to elicit more sensitive information—which cybercriminals then combine with the Private Information exposed in a data breach to commit substantial identity theft and fraud.

108. Plaintiff Bruce fears for her personal financial security and worries about what information was exposed in the Data Breach. Because of Defendant's Data Breach, Plaintiff Bruce has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Bruce's injuries are precisely the type of injuries that the law contemplates and addresses.

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

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

111. Plaintiff Bruce suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft that will continue for her lifetime—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

112. Because of the Data Breach, Plaintiff Bruce anticipates spending considerable amounts of time and money to try and mitigate her injuries.

113. Furthermore, Defendant's poor data security practices deprived Plaintiff Bruce of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, Plaintiff Bruce reasonably expected that Defendant would use reasonable data security to protect her Private Information (which Defendant required that Plaintiff disclose). Thus, when Defendant failed to provide reasonable data security, Plaintiff Bruce did not receive the full value of their bargain. After all, Plaintiff Bruce would have paid less for Defendant's products and/or services if Defendant was forthcoming about the inadequacy of its data security practices.

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

Plaintiff Gaifullin's Experiences and Injuries

115. Plaintiff Gaifullin is a former client of Defendant.

116. Thus, Defendant obtained and maintained Plaintiff's Private Information. As a result, Plaintiff Gaifullin's Private Information was exposed and exfiltrated by cybercriminals during Defendant's Data Breach.

117. As a condition of receiving products and/or services, Plaintiff Gaifullin provided Defendant with his Private Information. Defendant used that Private Information to facilitate its provision of products and/or services and to collect payment.

118. Plaintiff Gaifullin provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Gaifullin's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

119. Plaintiff Gaifullin is very careful about sharing his sensitive PII. Plaintiff Gaifullin takes proactive steps to ensure that his PII is kept safe and secure and would never knowingly transmit unencrypted sensitive PII over the internet. Thus, Plaintiff Gaifullin would not have entrusted his Private Information to Defendant if Defendant was transparent about its negligent data security practices.

120. Plaintiff Gaifullin reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

121. Plaintiff Gaifullin received a Notice of Data Breach in or around June 13, 2024.

122. Thus, on information and belief, Plaintiff Gaifullin's Private Information has already been published—or will be published imminently—and/or sold by cybercriminals on the Dark Web.

123. Plaintiff Gaifullin has ***already suffered*** from identity theft and fraud when cybercriminals attempted to hack into his PayPal account. While this occurred before May 2024, such fraudulent activity is nonetheless traceable to Defendant's Data Breach—which, upon information and belief, began earlier than Defendant has thus far determined and/or revealed.

124. Plaintiff Gaifullin has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Gaifullin to take those steps in its breach notice. This loss of time is significant and deprived Plaintiff Gaifullin of the opportunity to dedicate this time to recreation or to earn money through work.

125. And in the aftermath of the Data Breach, Plaintiff Gaifullin has suffered from a spike in spam and scam text messages and phone calls. This misuse of PII is traceable to Defendant's Data Breach because cybercriminals routinely obtain information (e.g., phone numbers and email addresses) which can be found online and then target data breach victims with scam calls and messages (i.e., phishing) to elicit more sensitive information—which cybercriminals then combine with the Private Information exposed in a data breach to commit substantial identity theft and fraud.

126. Plaintiff Gaifullin fears for his personal financial security and worries about what information was exposed in the Data Breach. Because of Defendant's Data Breach, Plaintiff Gaifullin has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Gaifullin's injuries are precisely the type of injuries that the law contemplates and addresses.

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

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

129. Plaintiff Gaifullin suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft that will continue for his lifetime—all because Defendant's Data Breach placed Plaintiff Gaifullin's Private Information right in the hands of criminals.

130. Because of the Data Breach, Plaintiff Gaifullin anticipates spending considerable amounts of time and money to try and mitigate his injuries.

131. Furthermore, Defendant's poor data security practices deprived Plaintiff Gaifullin of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, Plaintiff Gaifullin reasonably expected that Defendant would use reasonable data security to protect his Private Information (which Defendant required that Plaintiff Gaifullin disclose). Thus, when Defendant failed to provide reasonable data security, Plaintiff Gaifullin did not receive the full value of their bargain. After all, Plaintiff Gaifullin would have paid less for Defendant's products and/or services if Defendant was forthcoming about the inadequacy of its data security practices.

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

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

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

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

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

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

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

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

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

135. The value of Plaintiffs and Class's Private Information on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

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

137. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

138. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

139. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

140. Defendant disclosed the Private Information of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking,

unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

141. Defendant's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

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

142. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

143. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[30]

144. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[31]

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

---

[30] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

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

Defendant Failed to Follow FTC Guidelines.

146. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

147. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[32] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

148. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

149. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

[32] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

f. verify that third-party service providers use reasonable security measures.

150. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

151. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former clients' and customers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

152. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

153. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

154. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

155. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

156. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following "Nationwide Class":

> All individuals residing in the United States whose Private Information was accessed and/or acquired in the Data Breach discovered by Defendant in May 2024, including all those individuals who received notice of the Data Breach.

157. Plaintiffs also propose the following "Alabama Subclass," to be represented by Plaintiff William Colley:

> All individuals residing in Alabama whose Private Information was accessed and/or acquired in the Data Breach discovered by Defendant in May 2024, including all those individuals who received notice of the Data Breach.

158. Plaintiffs also propose the following "Florida Subclass," to be represented by Plaintiff Alice Bruce:

> All individuals residing in Florida whose Private Information was accessed and/or acquired in the Data Breach discovered by Defendant in May 2024, including all those individuals who received notice of the Data Breach.

159. Plaintiffs also propose the following "Pennsylvania Subclass," to be represented by Plaintiff Russell DeJulio:

> All individuals residing in Pennsylvania whose Private Information was accessed and/or acquired in the Data Breach discovered by Defendant in May 2024, including all those individuals who received notice of the Data Breach.

160. Plaintiffs also propose the following "Texas Subclass," to be represented by Plaintiff Efstathios Maroulis:

> All individuals residing in Texas whose Private Information was accessed and/or acquired in the Data Breach discovered by Defendant in May 2024, including all those individuals who received notice of the breach.

161. Together, the Nationwide Class and the State Subclasses are referred to as the "Class."

162. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

163. Plaintiffs reserve the right to amend the class definitions.

164. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

165. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

166. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Based upon notifications to states' attorneys general (such as the Maine Attorney General), the proposed Class includes at least 45,798 members.[33]

167. Typicality. Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

168. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including Interim Lead Class Counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

169. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Private Information;

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

c. if Defendant were negligent in maintaining, protecting, and securing PII in its possession and control;

[33] Data Breach Notification, MAINE ATTY GEN, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7d04d0f1-25d1-45b1-b1d0-87ba72a4d343.shtml (last accessed August 18, 2024)

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's Private Information;

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

f. if Defendant's Breach Notice was reasonable;

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

h. what the proper damages measure is; and

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

170. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

171. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

172. Plaintiffs and the Nationwide Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard and use it for business purposes only, and/or not disclose it to unauthorized third parties.

173. Defendant owed a duty of care to Plaintiffs and Nationwide Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would lead to the compromise of their Private Information in a data breach. And here, that foreseeable danger came to pass.

174. Defendant has full knowledge of the sensitivity of the Private Information it maintains, and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if such data was wrongfully disclosed.

175. Defendant owed these duties to Plaintiffs and Nationwide Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Nationwide Class Members' Private Information.

176. Defendant owed—to Plaintiffs and Nationwide Class Members—at least the following duties to:

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

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

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Nationwide Class Members within a reasonable timeframe of any breach to the security of their Private Information.

177. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Nationwide Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Nationwide Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

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

179. Defendant knew or reasonably should have known that the failure to exercise due care in the collection, storage, and use of Plaintiffs' and the Nationwide Class Members' Private Information involved an unreasonable risk of harm to them, even if the harm occurred through the criminal acts of a third party.

180. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

181. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Nationwide Class Members' Private Information.

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

183. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

184. The risk that unauthorized persons would attempt to gain access to Plaintiffs' and the Nationwide Class Members' Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII —whether by malware or otherwise.

185. PII – especially the types of PII at issue here – is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Nationwide Class Members' and the importance of exercising reasonable care in handling it.

186. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Nationwide Class by deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

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

188. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Nationwide Class Members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

189. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiffs and Nationwide Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Nationwide Class Members' injuries.

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

191. Defendant has admitted that the Private Information of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

192. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Nationwide Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

193. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—and/or sold by cybercriminals on the Dark Web.

194. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Nationwide Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

195. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

196. Plaintiffs and Nationwide Class Members were required to provide their Private Information to Defendant as a condition of receiving products/and or services provided by Defendant. Plaintiffs and Nationwide Class Members provided their Private Information to Defendant in exchange for Defendant's products/and or services.

197. Plaintiffs and Nationwide Class Members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

198. Plaintiffs and Nationwide Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were

required to provide based on Defendant's duties under state and federal law and its internal policies.

199. Plaintiffs and the Nationwide Class Members accepted Defendant's offers by disclosing their Private Information to Defendant in exchange for products/and or services.

200. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

201. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiffs' and Nationwide Class Member's Private Information and understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

202. Implicit in the agreement between Plaintiffs and Class Members and the 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, (f) retain the Private Information only under conditions that kept such information secure and confidential.

203. After all, Plaintiffs and Nationwide Class Members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

204. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

205. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

206. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

207. Defendant materially breached the contracts it entered with Plaintiffs and Nationwide Class Members by:

a. failing to safeguard their Private Information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

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

209. Defendant's material breaches of its implied contracts with Plaintiffs and Nationwide Class Members were the direct and proximate cause of Plaintiffs' and Nationwide Class Members' injuries, which injuries are alleged herein.

210. Plaintiffs and Nationwide Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

211. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

212. Plaintiffs and Nationwide Class Members conferred benefits upon Defendant. After all, Defendant benefitted from (1) accepting payment and/or commission from Plaintiffs and Nationwide Class Members, and (2) using their Private Information to facilitate its provision of products and/or services.

213. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Nationwide Class Members.

214. Plaintiffs and Nationwide Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

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

216. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Nationwide Class Members by utilizing cheaper, ineffective

security measures. Plaintiffs and Nationwide Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

217. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Nationwide Class Members' payment, commission, and/or Private Information because Defendant failed to adequately protect Plaintiffs' and Nationwide Class Members' Private Information.

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

219. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

220. 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) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) the compromised Private Information being disseminated and/or sold on the Dark Web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate measures to protect Private Information in its possession and control.

221. 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 the Plaintiffs and Class Members may seek restitution or compensation.

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

FOURTH CAUSE OF ACTION
Violation of the New York Deceptive Trade Practices Act ("DTPA")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Nationwide Class)

223. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

224. The DTPA provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." New York Gen. Bus. Law § 349(a).

225. Defendant violated DTPA by, *inter alia*:

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

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

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Nationwide Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Nationwide Class Members' Private Information; and

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

226. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their Private Information.

227. Defendant intended to mislead Plaintiffs and Nationwide Class Members and induce them to rely on its omissions.

228. Had Defendant disclosed to Plaintiffs and Nationwide Class Members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the Private Information that Plaintiffs and Nationwide Class Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Nationwide Class Members acted reasonably in

relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

229. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Nationwide Class Members' rights.

230. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiffs and the Class Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and, upon information and belief, available on the Dark Web for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

231. Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover their actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

232. Moreover, as a direct result of Defendant's violation of GBL § 349, Plaintiffs and Class Members are also entitled to injunctive relief, including, but not limited to, ordering Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

233. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

234. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

235. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Nationwide Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

236. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Nationwide Class Members.

237. The Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, including the following:

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

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

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

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to 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 Plaintiffs' and Class Members' Private Information;

v. requiring Defendant to engage independent third-party security

auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by 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;

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

ix. requiring Defendant to monitor ingress and egress of all network traffic;

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 Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring Defendant to implement a system of tests to assess its 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;

xii. requiring Defendant to implement, maintain, review, and revise as

necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

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

239. And if a third breach occurs, Plaintiffs and the Nationwide Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Nationwide Class Members' injuries.

240. If an injunction is not issued, the resulting hardship to Plaintiffs and Nationwide Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

241. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Nationwide Class Members, and the public at large.

SIXTH CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiffs Colley, DeJulio, Maroulis, and the Alabama, Pennsylvania, and Texas Subclasses)

242. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

243. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

245. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their Private Information.

246. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

247. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

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

249. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

250. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

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

SEVENTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs Bruce and Maroulis, and the Florida and Texas Subclasses)

252. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

253. Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

254. Defendant owed a duty to its current and former clients and customers, including Plaintiffs and the Florida and Texas Subclasses, to keep their Private Information confidential.

255. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Florida and Texas Subclasses Members' PII is highly offensive to a reasonable person.

256. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses were reasonable in their belief that such Private Information would be kept private and would not be disclosed without their authorization.

257. The Data Breach constitutes an intentional interference with Plaintiffs' Bruce and Maroulis and the Florida and Texas Subclasses' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

258. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

259. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

260. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses.

261. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses to suffer damages (as detailed *supra*).

262. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—and/or sold by cybercriminals on the Dark Web.

263. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Florida and Texas Subclasses since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

264. Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs Bruce and Maroulis and the Florida and Texas Subclasses.

265. In addition to injunctive relief, Plaintiffs Bruce and Maroulis, on behalf of themselves and the other Florida and Texas Subclasses Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

EIGHTH CAUSE OF ACTION
Violation of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. § 501.201, *et seq*.
(On Behalf of Plaintiff Alice Bruce and the Florida Subclass)

266. Plaintiffs incorporate by reference paragraphs 1 through 170 above as if fully set forth herein.

267. The purpose of FDUTPA is to "protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable,

deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

268. Another purpose of FDUTPA is to construe consumer protection as "consistent with established policies of federal law relating to consumer protection." Fla. Stat. § 501.202(3).

269. Plaintiff Bruce and Florida Subclass Members all constitute "consumers" under FDUTPA because they are all "individual[s]." Fla. Stat. § 501.203(7)

270. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

271. Plaintiff Bruce and Florida Subclass Members each constitute an "interested party or person" under FDUTPA because they are all "affected by a violation" of FDUTPA. Fla. Stat. § 501.203.

272. FDUTPA applies to Defendant because Defendant engages in "trade or commerce" in the State of Florida, which FDUPTA defines as "advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated." Fla. Stat. § 501.203.

273. FDUTPA declares unlawful "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

274. FDUTPA provides that "due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act." Fla. Stat. § 501.204(2).

275. Relevant here, is that "[v]iolation[s]" of FDUTPA are broadly defined to include violations of:

a. "Any rules promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. ss. 41 et seq." Fla. Stat. § 501.203.

b. "The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts." Fla. Stat. § 501.203.

c. "Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices." Fla. Stat. § 501.203.

276. Defendant violated FDUTPA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Florida Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

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

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bruce's and Florida Subclass Members'

PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Bruce's and Florida Subclass Members' Private Information; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bruce's and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 *et seq*.

277. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

278. Defendant intended to mislead Plaintiff Bruce and Florida Subclass Members and induce them to rely on its omissions.

279. Had Defendant disclosed to Plaintiff Bruce and Florida Subclass Members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the Private Information that Plaintiff Bruce and Florida Subclass Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Bruce and Florida Subclass Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

280. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff Bruce's and Florida Subclass Members' rights.

281. Plaintiff Bruce has standing to pursue this claim because as a direct and proximate result of Christie's violations of the FDUTPA, Plaintiff Bruce and the Florida Subclass have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Christie's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

282. Plaintiff Bruce also has standing to pursue this claim because, as a direct result of Christie's knowing violation of the FDUTPA, Plaintiff Bruce is at a substantial present and imminent risk of identity theft. Christie's still possesses Plaintiff Bruce's and the Florida Subclass's Private Information, and Plaintiff Bruce's Private Information has been potentially accessed by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiff and the Florida Subclass.

283. Plaintiff Bruce and the Florida Subclass are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Christie's engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Christie's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Christie's engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Christie's audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Christie's segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Christie's purge, delete, and destroy Private Information not necessary for its provisions of services in a reasonably secure manner;

f. ordering that Christie's to conduct regular database scans and security checks;

g. ordering that Christie's routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Christie's to meaningfully educate individuals about the threats they face as a result of the loss of their financial and Private Information to third parties, as well as the steps victims should take to protect themselves.

284. Plaintiff Bruce brings this action on behalf of herself and the Subclass for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow employees and consumers to make informed purchasing decisions and to protect Plaintiff Bruce, the Florida Subclass, and the public from Christie's unfair methods of competition and unfair, unconscionable, and unlawful practices. Christie's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

285. The above unfair, unconscionable, and unlawful practices and acts by Christie's were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Florida Subclass that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

286. Christie's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

287. Plaintiff Bruce and the Florida Subclass seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Christie's actions and/or practices violate the FDUTPA.

288. Plaintiff Bruce and the Florida Subclass are also entitled to recover the costs of this action (including reasonable attorneys' fees) and such other relief as the Court deems just and proper.

NINTH CAUSE OF ACTION
Wantonness
(On Behalf of Plaintiff Colley and the Alabama Subclass)

289. Plaintiffs incorporates by reference paragraphs 1 through 170 above as if fully set forth herein.

290. Defendant had the duty to use reasonable cybersecurity measures. But Defendant consciously failed to use reasonable cybersecurity measures to secure the Private Information of Plaintiff Colley and the Alabama Subclass. In other words, Defendant consciously acted to institute unreasonably insufficient cybersecurity measures.

291. Defendant was conscious that injury to Plaintiff Colley and the Alabama Subclass was the likely or probable result of its actions and omissions—regarding its failure to use reasonable cybersecurity, especially after suffering a prior data breach.

292. Defendant was recklessly indifferent to the consequences of its failure to use reasonable cybersecurity—and this reckless indifference left Plaintiff Colley's and the Alabama Subclass Private Information at risk of being accessed, exfiltrated, and/or sold by cybercriminals.

293. Defendant's conduct set forth herein was so reckless and so charged with indifference and conscious disregard to the consequences of its failure to exercise reasonable care in safeguarding and protecting Plaintiff Colley's and the Alabama Subclass Private Information as to amount to wantonness under Alabama law.

294. As a direct and proximate result of Defendant's wantonness, Plaintiff Colley and Alabama Subclass Members have suffered and will continue to suffer actual injuries-in-fact, and damages as a direct and/or proximate result of Defendant's failure to secure, safeguard and protect their Private Information in the form of, inter alia, (i) improper disclosure of their Private Information; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their Private Information, for which there is a well-established national and international market; and (vi) anxiety and emotional distress—for which they are entitled to compensation.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

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

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

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

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: August 19, 2024

Respectfully submitted,

/s/ Jon Mann

Jonathan S. Mann (admitted *pro hac vice*)
Chris T. Hellums*
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel.: (205) 322-8880
jonm@pittmandutton.com
chrish@pittmandutton.com

David K. Lietz (admitted *pro hac vice*)
Victoria Jennings Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440

Washington, D.C. 20015-2052
Tel.: (866) 252-0878
dlietz@milberg.com
vmaniatis@milberg.com

Courtney E. Maccarone
Mark S. Reich
Melissa Meyer
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Tel: (212) 363-7500
cmaccarone@zlk.com
mreich@zlk.com
mmeyer@zlk.com

Raina Borrelli (admitted *pro hac vice*)
Samuel J. Strauss*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago, IL 60611
Tel: (872) 63-1100
raina@straussborrelli.com
sam@straussborrelli.com

Jeff Ostrow (admitted *pro hac vice*)
Steven Sukert
KOPELOWITZ OSTROW P.A.
One West Las Olas Boulevard Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 900-2218
ostrow@kolawyers.com
sukert@kolawyers.com

Interim Lead Class Counsel for Plaintiffs and the Proposed Class

Mason Adams Barney
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue Suite 500
New York, NY 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Bruce W. Steckler*
STECKLER WAYNE & LOVE, PLLC
12720 Hillcrest Road, Suite 1045
Dallas, Texas 75230
Tel: (972) 387-4040
bruce@swclaw.com

Howard Theodore Longman
LONGMAN LAW, P. C.
521 Fifth Avenue Ste 17th Floor
New York, NY 10175
Tel: (973) 994-2315
hlongman@longman.law

Additional Attorneys for Plaintiffs and the Proposed Class

**Pro hac vice forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that on August 19, 2024, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will provide notification to all counsel of record.

/s/ Jon Mann
Of Counsel for Plaintiffs