Andrew G. Gunem (SBN 354042)
Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for the Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES

SUMNER DAVENPORT, DANIEL COHEN, and WILLIAM WOODWARD individually and on behalf of themselves and all others similarly situated, Plaintiffs, v. LA FINANCIAL FEDERAL CREDIT UNION, d/b/a LA FINANCIAL Defendant.	Case No.: 24-ST-CV-24021 **SECOND AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs Sumner Davenport, Daniel Cohen, and William Woodward ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant LA Financial Federal Credit Union, d/b/a LA Financial, ("LA Financial" or "Defendant") individually, on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. On information and belief, LA Financial discovered the Data Breach on June 10, 2024. Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to the personally identifiable information ("PII") of its current and former customers. The PII exposed includes, at least, the following:

a. names;

b. Social Security numbers;

c. financial account information; and

d. driver's license information.[1]

3. In or around September 11, 2024—three months after the Data Breach first occurred—LA Financial finally began notifying Class Members about the Data Breach ("Breach Notice"). As an example, Plaintiff Sumner Davenport's Breach Notice is attached as Exhibit A.

4. LA Financial took three months before informing Class Members even though Plaintiffs and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

[1] *Data Breach Notification Report*, MASS. OFF. CONSUM. AFFS. & BUS. REG., https://www.mass.gov/doc/data-breach-report-2024/download (last visited Nov. 21, 2024).

5. LA Financial's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its customers how many people were impacted, how the breach happened, when Defendant discovered the Breach, and why it took Defendant until September 11, 2024, to begin notifying victims that hackers had gained access to highly sensitive PII.

6. Defendant's failure to timely detect and report the Data Breach made its customers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

8. In failing to adequately protect Plaintiffs' and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former customers.

9. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiffs are Data Breach victims.

11. Accordingly, Plaintiffs, on behalf of themselves and a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

12. Plaintiff, Sumner Davenport, is a natural person and citizen of California, where she intends to remain. She is a Data Breach victim.

13. Plaintiff, Daniel Cohen, is a natural person and citizen of Oregon, where he intends to remain. He is a Data Breach victim.

14. Plaintiff, William Woodward, is a natural person and citizen of Arizona, where he intends to remain. He is a Data Breach victim.

15. Defendant, LA Financial Federal Credit Union, d/b/a LA Financial, is a credit union formed under the laws of California and with its principal place of business at 50 East Foothill Boulevard Suite 300, Arcadia California 91006.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10. This action is brought as a class action on behalf of Plaintiffs and Class Members pursuant to Cal. Code Civ. Proc. § 382.

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

18. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendant's principal office is in Los Angeles County, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in Los Angeles County.

STATEMENT OF FACTS

LA Financial

19. LA Financial is a California based credit union that touts "an 85-year history of putting our community first, serving members like you. Our 26,000+ members benefit from competitive rates and great products backed by local, friendly service."[2] LA Financial boasts a total annual revenue of $19 million.[3]

20. As part of its business, LA Financial receives and maintains the PII of thousands of current and former customers. In doing so, LA Financial implicitly promises to safeguard their PII.

21. In collecting and maintaining its current and former customers' PII, LA Financial agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

22. Indeed, Defendant acknowledges in its Privacy Policy that it "understands the importance of protecting your privacy" boasting that its goal is to "maintain your trust and confidence when handling your personal information."[4]

23. Defendant further assures its customers that it is "committed to maintaining the confidentiality of your personal information consistent with state and federal laws."[5]

---

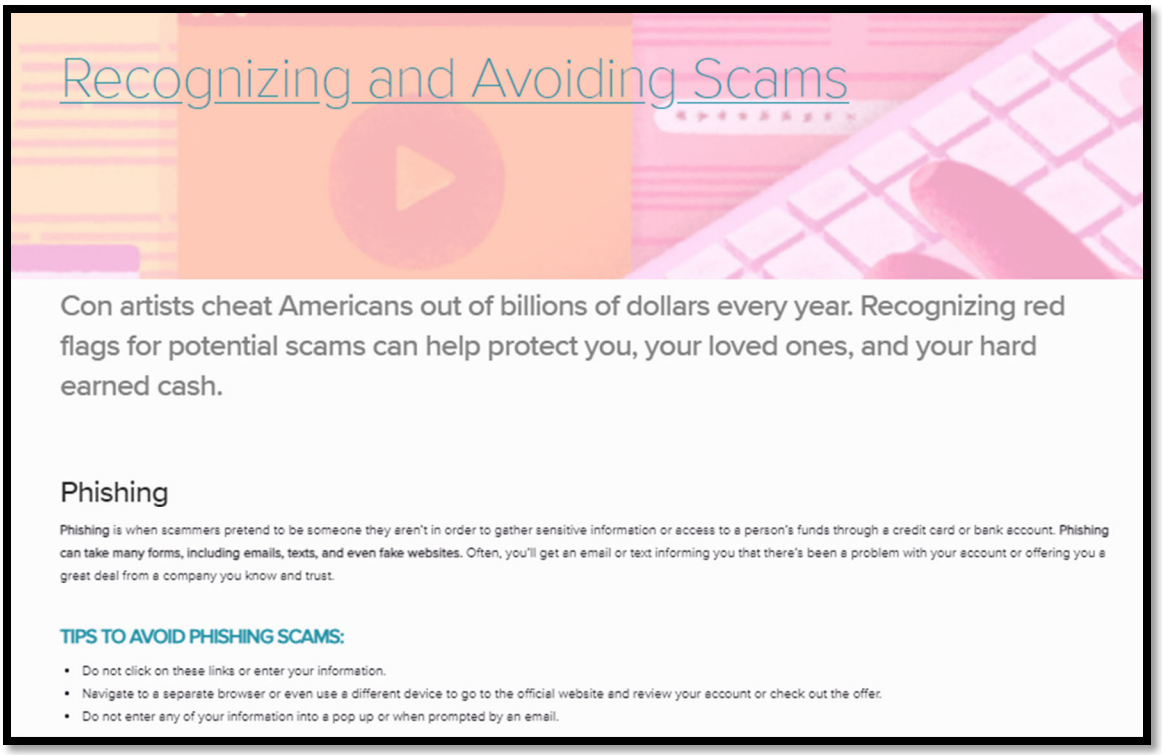
[2] *About us*, LA FINANCIAL, https://www.lafinancial.org/join-us/ (last visited September 12, 2024).

[3] *LA Financial*, ZOOMINFO, https://www.zoominfo.com/c/la-financial-credit-union/29115979, (last visited September 16, 2024).

[4] *Privacy Policy*, LA FINANCIAL, https://www.lafinancial.org/privacy-policy/ (last visited September 16, 2024).

[5] *Id*.

24. Indeed, so confident was Defendant in its cybersecurity and the importance of cybersecurity, that it regularly published articles advising its customers on how to best protect sensitive information, including blog articles on 'recognizing and avoiding scams', 'security tip[s]', and 'cybersecurity lessons':



Recognizing and Avoiding Scams

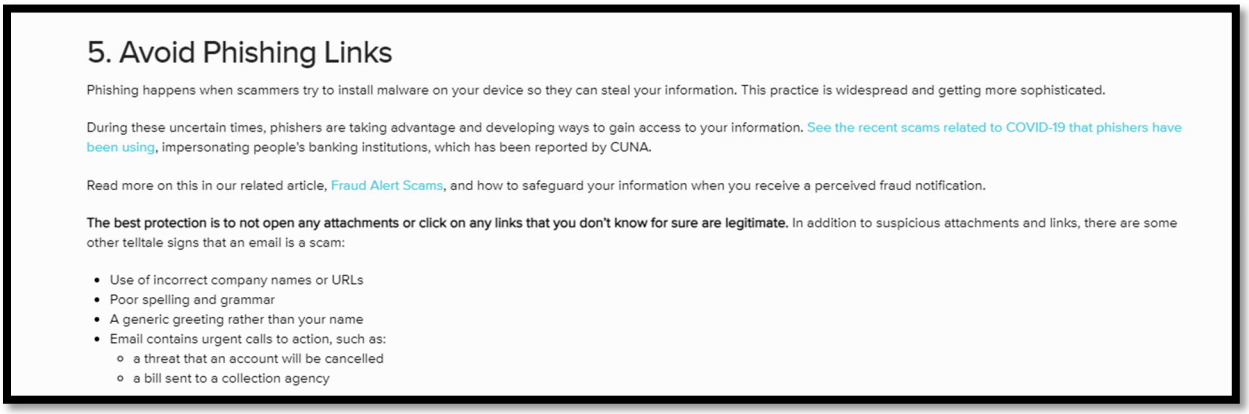
Con artists cheat Americans out of billions of dollars every year. Recognizing red flags for potential scams can help protect you, your loved ones, and your hard earned cash.

Phishing

Phishing is when scammers pretend to be someone they aren't in order to gather sensitive information or access to a person's funds through a credit card or bank account. **Phishing can take many forms, including emails, texts, and even fake websites.** Often, you'll get an email or text informing you that there's been a problem with your account or offering you a great deal from a company you know and trust.

TIPS TO AVOID PHISHING SCAMS:

- Do not click on these links or enter your information.
- Navigate to a separate browser or even use a different device to go to the official website and review your account or check out the offer.
- Do not enter any of your information into a pop up or when prompted by an email.



5. Avoid Phishing Links

Phishing happens when scammers try to install malware on your device so they can steal your information. This practice is widespread and getting more sophisticated.

During these uncertain times, phishers are taking advantage and developing ways to gain access to your information. See the recent scams related to COVID-19 that phishers have been using, impersonating people's banking institutions, which has been reported by CUNA.

Read more on this in our related article, Fraud Alert Scams, and how to safeguard your information when you receive a perceived fraud notification.

The best protection is to not open any attachments or click on any links that you don't know for sure are legitimate. In addition to suspicious attachments and links, there are some other telltale signs that an email is a scam:

- Use of incorrect company names or URLs
- Poor spelling and grammar
- A generic greeting rather than your name
- Email contains urgent calls to action, such as:
  - a threat that an account will be cancelled
  - a bill sent to a collection agency

25. Despite recognizing its duty to do so, on information and belief, LA Financial has not implemented reasonably cybersecurity safeguards or policies to protect its customers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, LA Financial leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to customers' PII.

The Data Breach

26. Plaintiffs and Class Members are current and former customers at Defendant.

27. In the course of their relationship, customers, including Plaintiffs and Class Members, provided Defendant with at least the following: names, Social Security numbers, and other sensitive information.

28. On information and belief, Defendant collects and maintains current and former customers' PII in its computer systems.

29. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

30. According to the Breach notice, "on or around June 10, 2024, [it] discovered suspicious activity potentially related to an email account". Following an internal investigation, LA Financial admitted that at least "one LA Financial employee email account was subject to unauthorized access." Ex. A.

31. In other words, Defendant's cyber and data security systems were completely inadequate in that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its customers' highly sensitive PII.

32. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's PII for theft and sale on the dark web.

33. Customers' place value in data privacy and security. These are important considerations when deciding who to bank with. Plaintiffs would not have accepted the Defendant's services, nor provided their PII, to Defendant had they known that LA Financial does not take all necessary precautions to secure the PII given to it by its customers.

34. In or around September 2024 –three months after the Breach was discovered– Defendant finally notified Plaintiffs and Class Members about the Data Breach.

35. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing its customers' PII, as evidenced by the Data Breach.

36. Typically, following the occurrence of a Data Breach, a company will announce that it is taking steps to enhance its existing security measures to prevent a similar event from occurring again. Not Defendant. Instead, Defendant puts the onus on Class members and makes no effort to assure its former and current customers about what it is doing to prevent a similar event from occurring again.

37. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity[.]" Ex. A.

38. Defendant also recognized through its Breach Notice, its duty to implement reasonable cybersecurity safeguards and policies to protect its customer's PII, insisting that, "we take the privacy and security of the information in our care very seriously and sincerely regret any worry or inconvenience this incident may cause you and your family." Ex. A.

39. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

40. On information and belief, LA Financial has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

41. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

42. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

43. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in Defendant's industry preceding the date of the breach.

44. In light of recent high profile data breaches, Defendant knew or should have known that its electronic records and customers' PII would be targeted by cybercriminals.

45. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).[6] The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).[7]

46. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

47. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [8]

48. Cyberattacks on companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller

[6] *ITRC Annual Data Breach Report*, ITRC, https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited Nov. 21, 2024).
[7] *Id.*
[8] *Gordon M. Snow Statement*, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited January 10, 2024).

municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

49. 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.

PLAINTIFFS' EXPERIENCES

Plaintiff Sumner Davenport's Experience

50. Plaintiff Sumner Davenport is a current customer of Defendant.

51. As a condition of receiving services, Defendant required that Plaintiff disclose her PII. Defendant used that PII to facilitate its provision of services to Plaintiff and to collect payment for such services.

52. Plaintiff provided her PII to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

53. Plaintiff received an official notice letter of the Data Breach from Defendant.

54. Defendant deprived Plaintiff of the earliest opportunity to guard against the Data Breach's effects by failing to notify her about it for three months.

55. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

56. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She does not knowingly transmit her unencrypted sensitive PII over the internet in an unsecure manner. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

[9] *Secret Service Warn of Targeted*, LAW360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited January 10, 2024).

57. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her financial and credit accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

58. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect themselves from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

59. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

60. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised by the Data Breach.

61. Plaintiff suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of cybercriminals.

62. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

63. In sum, Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (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) nominal damages; and (viii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

Plaintiff Daniel Cohen's Experience

64. Plaintiff Daniel Cohen is a former customer of Defendant.

65. As a condition of receiving services, Defendant required that Plaintiff disclose his PII. Defendant used that PII to facilitate its provision of services to Plaintiff and to collect payment for such services.

66. Plaintiff provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

67. Plaintiff received an official notice letter of the Data Breach from Defendant.

68. Defendant deprived Plaintiff of the earliest opportunity to guard against the Data Breach's effects by failing to notify him about it for three months.

69. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

70. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. She does not knowingly transmit his unencrypted sensitive PII over the internet in an unsecure manner. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

71. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his financial and credit accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

72. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect themselves from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

73. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

74. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised by the Data Breach.

75. Plaintiff suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of cybercriminals.

76. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

77. In sum, Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (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) nominal damages; and (viii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

78. Plaintiff further suffered actual injury in the form of his PII being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

79. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

Plaintiff Woodward's Experience

80. Plaintiff Woodward is a former customer of Defendant.

81. As a condition of receiving services, Defendant required that Plaintiff disclose his PII. Defendant used that PII to facilitate its provision of services to Plaintiff and to collect payment for such services.

82. Plaintiff provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

83. Plaintiff received an official notice letter of the Data Breach from Defendant.

84. Defendant deprived Plaintiff of the earliest opportunity to guard against the Data Breach's effects by failing to notify him about it for three months.

85. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

86. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. She does not knowingly transmit his unencrypted sensitive PII over the internet in an unsecure manner. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

87. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his financial and credit accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

88. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect themselves from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

89. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere

worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

90. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised by the Data Breach.

91. Plaintiff suffered imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of cybercriminals.

92. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

93. In sum, Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (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) nominal damages; and (viii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

94. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

95. 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.

96. The value of Plaintiffs' and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

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

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

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

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

101. Defendant disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class 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 PII.

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

Defendant failed to adhere to FTC guidelines.

103. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

104. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII 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.

105. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

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

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

Defendant Fails to Comply with Industry Standards

109. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

110. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

111. Other best cybersecurity practices that are standard for employers 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

112. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

113. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its customers. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Failed to Comply with the Gramm-Leach-Bliley Act

114. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

115. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

116. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

117. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

118. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

119. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention

to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

120. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

121. Defendant failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

122. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security

program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

123. As alleged herein, Defendant violated the Safeguard Rule.

124. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

125. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members with a non-affiliated third party without providing Plaintiffs and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendant Fails To Comply With Industry Standards

126. As noted above, experts studying cyber security routinely identify financial institutions in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

127. Several best practices have been identified that, at a minimum, should be implemented by financial institutions in possession of PII, like Defendant, including but not

limited to: 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

128. Other best cybersecurity practices that are standard for financial institutions 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

129. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

130. These foregoing frameworks are existing and applicable industry standards for financial institutions, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

131. Plaintiffs, on behalf of themselves, and all others similarly situated pursuant to California's Class Action Mechanism (Cal. Civ., § 382) bring this nationwide class action for the following "Nationwide Class" defined as:

> All individuals residing in the United States whose PII was compromised in the Data Breach, including all those who received notice of the breach.

132. Plaintiff William Woodward also proposes the following "Arizona Subclass" to be represented by Plaintiff William Woodward:

> All individuals residing in Arizona whose PII was compromised in the Data Breach, including all those who received notice of the breach.

133. Plaintiff Daniel Cohen also proposes the following "Oregon Subclass" to be represented by Plaintiff Daniel Cohen:

> All individuals residing in Oregon whose PII was compromised in the Data Breach, including all those who received notice of the breach.

134. Together, the Nationwide Class, Arizona Subclass, and Oregon Subclass are referred to as the "Class."

135. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

136. Plaintiffs reserve the right to amend the class definition.

137. 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.

138. **Numerosity**. Plaintiffs are representative of the Class, consisting of several thousand members, far too many to join in a single action;

139. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

140. **Typicality**. Plaintiffs' claims are typical of class 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.

141. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

142. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

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

c. Whether Defendant were negligent in maintaining, protecting, and securing PII;

d. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

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

f. Whether Defendant's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

h. What the proper damages measure is; and

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

143. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual Plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

144. Plaintiffs reallege all previous paragraphs as if fully set forth below.

145. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

146. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance

with state-of-the-art industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

147. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class 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.

148. Defendant owed these duties to Plaintiffs and members of the Class 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 protocols. Defendant actively sought and obtained Plaintiffs' and the Class's PII.

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

150. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and the Class and the importance of exercising reasonable care in handling it.

151. 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 PII of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

153. Plaintiffs reallege all previous paragraphs as if fully set forth below.

154. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

155. 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 customers or, in this case, customers' PII. 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 members of the Class's PII.

156. Defendant breached its 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 PII.

157. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

158. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's 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 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.

159. 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 the Class.

160. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

161. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it 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.

162. Had Plaintiffs and the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

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

164. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

165. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

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

166. Plaintiffs reallege all previous paragraphs as if fully set forth below.

167. Plaintiffs and the Class delivered their PII to Defendant as part of the process of obtaining banking services from Defendant.

168. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

169. In providing their PII, Plaintiffs and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' PII.

170. In delivering their PII to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard that data.

171. Plaintiffs and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

172. Defendant accepted possession of Plaintiffs' and Class Members' PII.

173. Had Defendant disclosed to Plaintiffs and Class Members that Defendant did not have adequate computer systems and security practices to secure customers' PII, Plaintiffs and members of the Class would not have provided their PII to Defendant.

174. Defendant recognized that customers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

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

176. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard its data.

177. Defendant breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

178. As a direct and proximate result of the breach of contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of their PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft

and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiffs and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiffs' and Class Members' PII.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

179. Plaintiffs reallege all previous paragraphs as if fully set forth below.

180. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

181. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

182. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's PII, as this was used to facilitate the services and goods it sold to Plaintiffs and the Class.

183. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the Class's PII because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII to Defendant had they known Defendant would not adequately protect their PII.

184. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Invasion of Privacy
Cal. Const. ART. 1 § 1
(On Behalf of Plaintiffs and the Class)

185. Plaintiffs reallege all previous paragraphs as if fully set forth below.

186. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

187. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

188. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

189. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

190. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

191. Defendant knowingly did not notify Plaintiffs' and Class Members in a timely fashion about the Data Breach.

192. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

193. As a proximate result of Defendant's acts and omissions, the PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

194. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

195. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their PII. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

196. Plaintiffs and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

197. Plaintiffs and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(On Behalf of Plaintiffs and the Class)

198. Plaintiffs reallege all previous paragraphs as if fully set forth below.

199. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

200. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

201. Defendant stored the PII of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs' and the Class's PII secure so as to prevent the loss or misuse of that PII.

202. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure. However, Plaintiffs and the Class were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiffs and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

203. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the Class's nonencrypted and nonredacted PII.

204. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

205. Defendant's conduct was unlawful, in that it violated the CCPA.

206. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

207. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

208. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

209. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

210. Instead, Defendant made the PII of Plaintiffs and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

211. As a result of those unlawful and unfair business practices, Plaintiffs and the Class suffered an injury-in-fact and have lost money or property.

212. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

213. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

214. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VII
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiffs and the Class)

215. Plaintiffs reallege all previous paragraphs as if fully set forth below.

216. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs', and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

217. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

218. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiffs' and Class members' PII. Plaintiffs and Class members have

an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

219. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiffs believes such cure is not possible under these facts and circumstances—then Plaintiffs intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

220. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

221. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

COUNT VIII
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

222. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

223. Under California law, every contract imposes on each party a duty of good faith and fair dealing in each performance and its enforcement. 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.

224. 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.

225. Here, Plaintiffs and Defendant entered into a contract (implied in law, fact, or otherwise) whereby Defendant agreed to: (a) use a portion of the funds paid by Plaintiffs and Class Members to pay for adequate cybersecurity measures; (b) use adequate cybersecurity measures as required by state law, federal law, and Defendant's contractual agreements (implied or otherwise); and (c) notify them promptly of any exposure of their PII.

226. As current and former employees, Plaintiffs and Class Members fully fulfilled their contractual obligations when they paid Defendant.

227. Furthermore, the conditions precedent (if any) to Defendant's performance have already occurred.

228. Defendant unfairly interfered with the Plaintiffs' and Class Members' rights to receive the benefits of the contract—and breached the covenant of good faith and fair dealing—by, *inter alia*: (a) failing to safeguard their 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 its legal obligations; and (e) failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

229. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

COUNT IX
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

230. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

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

232. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

233. Because of the highly sensitive nature of the PII, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

234. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII.

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

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

COUNT X
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiffs and the Class)

237. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

238. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, ***or*** is reasonably believed to have been, acquired by an unauthorized person." *Id* (emphasis added).

239. The Data Breach constitutes a "breach of the security system" of Defendant.

240. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class.

241. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class but waited approximately three months to notify them. Given the severity of the Data Breach, three months was an unreasonable delay.

242. Defendant's unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

243. Because Plaintiffs and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

244. Plaintiffs and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT XI
Violation of the Arizona Consumer Fraud Act
A.R.S. §§ 44-1521, *et seq*.
(On Behalf of Plaintiff William Woodward and the Arizona Subclass)

245. Plaintiff William Woodward incorporates by reference all other paragraphs as if fully set forth herein.

246. Under A.R.S. § 44-1521, Defendant's products and services are "merchandise" because they are "objects, wares, goods, commodities, intangibles, real estate or services."

247. Defendant violated Arizona Consumer Fraud Act by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Arizona Subclass Members' PII, 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's and Arizona Subclass Members' PII,

including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *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's and Arizona Subclass Members' PII; 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's and Arizona Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

248. 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.

249. Defendant intended to mislead Plaintiff and Arizona Subclass Members and induce them to rely on its omissions.

250. Had Defendant disclosed to Plaintiff and Arizona Subclass Members (or their third-party agents) 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 PII that Plaintiff and Arizona Subclass Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Arizona

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

251. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Arizona Subclass Members' rights.

252. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

253. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

254. Plaintiff and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law.

COUNT XII
Violation of the Oregon Unlawful Trade Practices Act
(On Behalf of Plaintiff Daniel Cohen and the Oregon Subclass)

255. Plaintiff Daniel Cohen incorporates by reference all other paragraphs as if fully set forth herein.

256. Plaintiff, Oregon Subclass Members, and Defendant are all persons under the Oregon Unlawful Trade Practices Act ("UTPA"), Ore. Stat. § 646.605(4). Defendants engaged in "trade" or "commerce" under Ore. Stat. § 646.605(8). The UTPA prohibits all "unfair or deceptive" conduct in trade or commerce under Ore. Stat. § 646.608(1), which includes the conduct complained of herein.

257. Defendant violated Oregon Unlawful Trade Practices Act by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Oregon Subclass Members' PII, 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's and Oregon Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *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's and Oregon Subclass Members' PII; 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's and Oregon Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

258. 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.

259. Defendant intended to mislead Plaintiff and Oregon Subclass Members and induce them to rely on its omissions.

260. Had Defendant disclosed to Plaintiff and Oregon Subclass Members (or their third-party agents) 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 PII that Plaintiff and Oregon Subclass Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Oregon Subclass Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

261. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Oregon Subclass Members' rights.

262. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Oregon Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

263. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

264. Plaintiff and Oregon Subclass Members seek all monetary and non-monetary relief allowed by law.

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request 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 is necessary to protect the interests of Plaintiffs and the Class;

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

D. Enjoining Defendant from further deceptive practices and making untrue statements Plaintiffs the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include 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 such other or further relief as may be appropriate under the circumstances.

Dated: November 29, 2024

By: */s/ Andrew G. Gunem*

Andrew G. Gunem (SBN 354042)
Samuel J. Strauss*
Raina Borelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1110
agunem@straussborrelli.com
sam@straussborrelli.com
raina@straussborrelli.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
jnelson@milberg.com

John P. Kristensen (SBN 224132)
KRISTENSEN LAW GROUP
120 Santa Barbara St., Suite C9
Santa Barbara, California 93101
Telephone: (805) 837-2000
john@kristensen.law

Jarrett Ellzey*
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455
jellzey@eksm.com

**Pro hac vice forthcoming*
Attorneys for Plaintiffs and Proposed Class