**UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF NORTH CAROLINA**
**CHARLOTTE DIVISION**

| | |
|---|---|
| **GEORGE MARDIKIAN**, on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>**FIGURE LENDING LLC** d/b/a **FIGURE**,<br><br>Defendant. | **No. 3:26-cv-00135**<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

George Mardikian ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Figure Lending LLC d/b/a Figure ("Figure" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his 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 blockchain-based financial technology company transforming capital markets and is the nation's largest non-bank provider of home equity lines of credit.[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its customers. But Defendant lost control over that data when

[1] *Overview*, FIGURE, https://www.linkedin.com/company/figuretechnologies/about/ (last visited Feb. 19, 2026).

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 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 customers' PII.

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 PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim. He brings this Class Action on behalf of himself, 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, its customers' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

## PARTIES

8. Plaintiff, George Mardikian, is a natural person and a citizen of Merced, California. He is domiciled in California (where he intends to remain).

9. Defendant Figure is a foreign Limited Liability Company incorporated in Delaware and with its principal place of business at 650 South Tryon Street, 8th Floor, Charlotte, North Carolina 28202.

## JURISDICTION AND VENUE

10. 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. Plaintiff and Defendant are citizens of different states.[2] And there are over 100 putative Class Members.

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

12. 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 Plaintiff's claims occurred in this District.

## BACKGROUND

***Defendant Collected and Stored the PII of Plaintiff and the Class***

13. Defendant is a blockchain-based financial technology company transforming capital markets and is the nation's largest non-bank provider of home equity lines of credit.[3]

14. As part of its business, Defendant receives and maintains the PII of thousands of its customers.

[2] Under the Class Action Fairness Act, "an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized." 28 U.S.C. § 1332(d)(10); Thus, as an LLC, Defendant Figure is a citizen of Delaware (state of formation) and North Carolina (principal place of business).

[3] *Overview*, FIGURE, https://www.linkedin.com/company/figuretechnologies/about/ (last visited Feb. 19, 2026).

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

16. Under state and federal law, businesses like Defendant's have duties to protect their customers' PII and to notify them about breaches.

17. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "We use reasonable precautions, including technical and administrative measures, to protect your Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction."[4]

b. "We want to be clear that we do not sell your Personal Data to any other entities. Data obtained through the SMS messaging program will not be shared with any third parties for their marketing reasons/purposes."[5]

c. "We are committed to respecting your privacy choices and handling your data responsibly."[6]

***Defendant's Data Breach***

18. On or about February 14, 2026, Defendant was hacked in the Data Breach.[7]

[4] *Privacy Policy*, FIGURE, https://www.figure.com/privacy/ (last visited Feb. 19, 2026).
[5] *Id*.
[6] *Id*.
[7] *Overview: Figure.com Data Breach*, UPGUARD, https://www.upguard.com/news/figure-data-breach-2026-02-16 (last visited Feb. 19, 2026).

19. Worryingly, Defendant already admitted that it experienced a data breach and that "the breach originated when an employee was tricked with a social engineering attack that allowed the hackers to steal 'a limited number of files.'"[8]

20. Because of Defendant's Data Breach, at least the following types of PII[9] were compromised:

a. Customer's full names;

b. Home addresses;

c. Dates of birth; and

d. Phone numbers.

21. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative Class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative Class is over thousands of members—as it includes its customers.

22. And yet, Defendant has yet to notify the Class.

23. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

24. Notably, California Civ. Code § 1798.82(a)(2)(A) mandates that notice "shall be made within 30 calendar days of discovery or notification of the data breach."

25. 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

[8] *Fintech lending giant Figure confirms data breach,* TECHCRUNCH, https://techcrunch.com/2026/02/13/fintech-lending-giant-figure-confirms-data-breach/ (last visited Feb. 19, 2026).
[9] *Id*.

Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

26. Since the Data Breach, Defendant claims that "the attackers obtained a limited number of files," and Defendant offered "free credit monitoring 'to all individuals who receive a notice.'"[10]

27. But such simple declarations are insufficient to ensure that Plaintiff's and Class Members' PII will be protected from additional exposure in a subsequent data breach.

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

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

***ShinyHunters & the Dark Web***

30. Worryingly, the cybercriminals that obtained Plaintiff's and Class Members' PII appear to be the notorious cybercriminal group "ShinyHunters."[11]

[10] *Id.*

[11] *Data breach at fintech giant Figure affects close to a million customers*, TECHCRUNCH, https://techcrunch.com/2026/02/18/data-breach-at-fintech-giant-figure-affects-close-to-a-million-customers/ (last visited Feb. 19, 2026).

31. ShinyHunters is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) released a FLASH Alert warning the public about ShinyHunters.[12] Specifically, the FBI stated, *inter alia*, that:

a. "The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate Indicators of Compromise (IOCs) associated with recent malicious cyber activities by cyber criminal groups UNC6040 and UNC6395, responsible for a rising number of data theft and extortion intrusions."[13]

b. "Both groups have recently been observed targeting organizations' Salesforce platforms via different initial access mechanisms."[14]

c. "The FBI is releasing this information to maximize awareness and provide IOCs that may be used by recipients for research and network defense."[15]

d. "Some UNC6040 victims have subsequently received extortion emails allegedly from the ShinyHunters group, demanding payment in cryptocurrency to avoid publication of exfiltrated data. These extortion demands have varied in time following UNC6040 threat actors' access and data exfiltration, ranging from a period of days to months."[16]

[12] *Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion*, FBI FLASH, https://www.ic3.gov/CSA/2025/250912.pdf (last visited Feb. 19, 2026).
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] *Id*.

32. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully acquired data.

33. Worryingly, the "hacking group ShinyHunters took responsibility for the hack on its official dark web leak website, saying the company refused to pay a ransom, and published 2.5 gigabytes of allegedly stolen data."[17] In addition, "TechCrunch saw a portion of the data, which included customers' full names, home addresses, dates of birth, and phone numbers."[18]

34. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the dark web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[19]

35. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the dark web.

***Plaintiff's Experiences and Injuries***

36. Plaintiff George Mardikian has had an active loan with Defendant for about three (3) years.

37. Thus, Defendant obtained and maintained Plaintiff's PII.

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

---

[17] *Fintech lending giant Figure confirms data breach,* TECHCRUNCH, https://techcrunch.com/2026/02/13/fintech-lending-giant-figure-confirms-data-breach/ (last visited Feb. 19, 2026).

[18] *Id.*

[19] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

39. Plaintiff is very careful about the privacy and security of his PII. He does not knowingly transmit his PII over the internet in an unsafe manner. He is careful to store any documents containing his PII in a secure location.

40. Plaintiff provided his PII 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 PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

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

42. Through its Data Breach, Defendant compromised Plaintiff's PII.

43. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

44. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls.

45. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

46. Because of Defendant's Data Breach, Plaintiff 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's injuries are precisely the type of injuries that the law contemplates and addresses.

47. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

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

49. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

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

51. Today, 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 additional breaches.

***Consumers Prioritize Data Security***

52. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[20] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[21]

[20] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[21] *Id*. at 3.

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[22]

c. 89% of consumers stated that "I care about data privacy."[23]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[24]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[25]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[26]

***Plaintiff and the Proposed Class Suffered Common Injuries and Damages***

53. Because of Defendant's failure to prevent the Data Breach, Plaintiff 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 PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

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

[22] *Id*.
[23] *Id*. at 9.
[24] *Id*.
[25] *Id*.
[26] *Id*. at 11.

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 identity theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—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 PII.

***Substantially Increased Risk of Identity Theft and Fraud***

54. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

55. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

56. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

57. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the dark web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

58. The "dark web" is an unindexed layer of the internet that requires special software or authentication to access.[27] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[28] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

59. The unencrypted PII of Plaintiff and Class Members has or will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

60. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

61. In particular, the theft of Social Security numbers—in combination with other PII (e.g., name, address, date of birth)—provides cybercriminals with a "skeleton key" to commit rampant fraud and identity theft.

62. For example, cybersecurity expert Jim Stickley explained to Time Magazine that "[i]f I have your name and your Social Security number, and you haven't gotten a credit freeze

[27] *What Is the Dark Web?*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited July 9, 2025).
[28] *Id.*

yet, you're easy pickings . . . With that, you can do whatever you want . . . You can become that person."[29] For context, Jim Stickley is a "penetration tester" who is employed by businesses "to infiltrate their systems in order to find flaws they can fix before the bad guys exploit them."[30]

63. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

64. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[31]

65. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

66. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

---

[29] Patrick L. Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME MAGAZINE (Aug. 5, 2019) https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[30] *Id.*
[31] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. SYSTEMICS, CYBERNETICS & INFORMATICS 9 (2019) http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

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

68. Identity thieves can also use an individual's personal data and PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[32]

69. One example of criminals piecing together bits and pieces of compromised PII to create comprehensive dossiers on individuals is called "Fullz" packages.[33] These dossiers are both

[32] *Identity Theft and Your Social Security Number,* SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited July 9, 2025).

[33] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone

shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals 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 to assemble complete dossiers on individuals. For example, they can combine the stolen PII, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

70. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet. 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 Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

71. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[34]

---

with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm,* KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

[34] *2019 Internet Crime Report* (Feb. 11, 2020) FED. BUREAU INTELLIGENCE, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited July 9, 2025).

72. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Yet, Defendant failed to rapidly report to Plaintiff and the Class that their PII was stolen. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injuries 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.

73. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

74. In addition to out-of-pocket expenses that can exceed thousands of dollars, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

75. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

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

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

77. In 2024, a record 3,158 data breaches occurred—exposing approximately

1,350,835,988 sensitive records (i.e., 211% increase year over year).[35]

78. 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."[36]

79. 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.

***Defendant Could Have Prevented the Data Breach***

80. Data breaches are preventable.[37] Indeed, the American Bar Association published a treatise titled the *Data Breach and Encryption Handbook* wherein the author explained that:

a. "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[38]

b. "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[39]

---

[35] *2024 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.
[36] 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.
[37] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (2012).
[38] *Id.* at 17.
[39] *Id.* at 28.

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

***Defendant Failed to Follow FTC Guidelines***

81. 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.

82. 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.[41] 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.

83. 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.

---

[40] *Id.*

[41] *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.

84. 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

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

85. 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.

86. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its 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***

87. 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.

88. 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.

89. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

90. 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.

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

91. 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.

92. 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).

93. 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 was 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.

94. 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.

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

96. Both the Privacy Rule and Regulation P require financial institutions to provide consumers 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.

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

98. Defendant failed to adequately inform their consumers that it was storing and/or sharing, or would store and/or share, the consumers' PII on an insecure platform, accessible to unauthorized parties, and would do so after the relationship ended.

99. 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 consumer 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 consumer 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 consumer 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.

100. As alleged herein, Defendant violated the Safeguards Rule.

101. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of consumer information.

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

## CLASS ACTION ALLEGATIONS

103. Plaintiff brings 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 classes:

> **Nationwide Class**
> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Figure in February 2026, including all those individuals who received notice of the breach.
> **California Subclass**
> All individuals residing in California whose PII was compromised in the Data Breach discovered by Figure in February 2026, including all those individuals who received notice of the breach.

Collectively, the Nationwide Class and California Subclass are referred to as the "Class", and the individuals in the Class are referred to as "Class Members."

104. 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.

105. Plaintiff reserves the right to amend the Class definition.

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

107. 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.

108. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least thousands of members.

109. Typicality. Plaintiff's 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.

110. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex Class Action litigation and data privacy to prosecute this action on the Class's behalf.

111. Commonality and Predominance. Plaintiff's 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 Plaintiff's and the Class's PII;

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 was negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

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 Plaintiff and the Class injuries;

h. what the proper damages measure is; and

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

112. 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 Plaintiff and the Class)**

113. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

114. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

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

116. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

117. Defendant owed these duties to Plaintiff and 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 Plaintiff and Class Members' PII.

118. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII 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 Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

119. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required

and necessary for Plaintiff and 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.

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

121. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

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

123. Similarly, and as described *supra*, Defendant violated its duties under the GLBA, 15 U.S.C. § 6809(3)(A) which constitutes negligence.

124. Similarly, and as described *infra*, Defendant violated its duties under the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*. (the "CRA"), and other state data security laws which constitutes negligence.

125. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold 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.

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

127. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

129. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

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

b. 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.

130. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

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

132. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

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

134. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

135. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members 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.

## SECOND CAUSE OF ACTION
**Negligence *per se***
**(On Behalf of Plaintiff and the Class)**

136. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

137. 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 Plaintiff's and Class Members' PII.

138. 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 Plaintiff and the Class Members' sensitive PII.

139. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

140. 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.

141. 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 Plaintiff and members of the Class.

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

143. The injury and harm suffered by Plaintiff 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 Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

144. Similarly, and as described *supra*, Defendant violated its duties under the GLBA, 15 U.S.C. § 6809(3)(A) which constitutes negligence *per se*.

145. Similarly, and as described *infra*, Defendant violated its duties under the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), the California

Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*. (the "CRA"), and other state data security laws which constitutes negligence *per se*.

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

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

**THIRD CAUSE OF ACTION**
**Breach of Implied Contract**
**(On Behalf of Plaintiff and the Class)**

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's services.

150. Plaintiff and Class Members reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

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

152. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for services.

153. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

154. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

155. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

156. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

157. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

158. 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.

159. 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.

160. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

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 the legal obligations necessarily incorporated into the agreements; and

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

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

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

163. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

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

## FOURTH CAUSE OF ACTION
### Invasion of Privacy
### (On Behalf of Plaintiff and the Class)

165. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

166. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

167. Defendant owed a duty to its customers, including Plaintiff and the Class, to keep this information confidential.

168. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

169. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did

so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

170. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's 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.

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

172. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

173. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

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

175. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

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

177. Plaintiff and the Class 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 PII of Plaintiff and the Class. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks 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.

## FIFTH CAUSE OF ACTION
**Unjust Enrichment**
**(On Behalf of Plaintiff and the Class)**

178. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

179. This claim is pleaded in the alternative to the breach of implied contract claim.

180. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII to provide services, and (2) accepting payment.

181. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

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

183. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

184. 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures.

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

185. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII and (2) payment because Defendant failed to adequately protect their PII.

186. Plaintiff and Class Members have no adequate remedy at law.

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

## SIXTH CAUSE OF ACTION
**Breach of Fiduciary Duty**
**(On Behalf of Plaintiff and the Class)**

188. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

189. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff 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.

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

191. Because of the highly sensitive nature of the PII, Plaintiff 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.

192. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

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

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

## SEVENTH CAUSE OF ACTION
**Declaratory Judgment**
**(On Behalf of Plaintiff and the Class)**

195. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

196. 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.

197. 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, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

198. 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 Plaintiff and Class Members.

199. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

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

201. And if a second breach occurs, Plaintiff and the 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 Plaintiff and Class Members' injuries.

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

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

**EIGHTH CAUSE OF ACTION**
**Violation of California's Unfair Competition Law (UCL)**
**Cal. Bus. & Prof. Code § 17200, *et seq*.**
**(On Behalf of Plaintiff and the California Subclass)**

204. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

205. 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").

206. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*. (the "CRA"), and other state data security laws.

207. Defendant stored the PII of Plaintiff and the California Subclass 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 Plaintiff's and the California Subclass's PII secure to prevent the loss or misuse of that PII.

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

209. 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 Plaintiff's and the California Subclass's nonencrypted and nonredacted PII.

210. Had Defendant complied with these requirements, Plaintiff and the California Subclass would not have suffered the damages related to the data breach.

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

212. 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.

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

214. 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.

215. Defendant also engaged in unfair business practices under the "tethering test." Defendant's 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.

216. Instead, Defendant made the PII of Plaintiff and the California Subclass accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the California Subclass 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.

217. As a result of those unlawful and unfair business practices, Plaintiff and the California Subclass suffered an injury-in-fact and have lost money or property.

218. For one, on information and belief, Plaintiff's and the California Subclass's stolen PII has already been published—or will be published imminently—by cybercriminals on the dark web.

219. The injuries to Plaintiff and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

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

221. Therefore, Plaintiff and the California Subclass 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.

## NINTH CAUSE OF ACTION
**Violations of the California Consumer Privacy Act ("CCPA")**
**Cal. Civ. Code § 1798.150**
**(On Behalf of Plaintiff and the California Subclass)**

222. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

223. Defendant violated the CCPA by failing to provide timely notice—whereas the CCPA requires disclosure "within 30 calendar days of discovery or notification of the data breach." Cal. Civ. Code § 1798.82(a)(2)(A).

224. 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 Plaintiff and the California Subclass. As a direct

and proximate result, Plaintiff's and the California Subclass's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

225. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civ. Code § 1798.140(d).

226. Plaintiff and California Subclass 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 Plaintiff's and California Subclass Members' PII. Plaintiff and California Subclass 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.

227. Pursuant to California Civil Code § 1798.150(b), Plaintiff 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 Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

228. 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.

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

## TENTH CAUSE OF ACTION
**Violation of the California Customer Records Act**
**Cal. Civ. Code § 1798.80, *et seq*.**
**(On Behalf of Plaintiff and the California Subclass)**

230. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

231. 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).

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

233. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the California Subclass.

234. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the California Subclass failed to notify them. Given the severity of the Data Breach, it was unreasonable to delay notice.

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

236. Because Plaintiff and the California Subclass were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

237. Plaintiff and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

**PRAYER FOR RELIEF**

Plaintiff 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 Plaintiff and the proposed Class, appointing Plaintiff as Class representative, and appointing his counsel to represent the Class;

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

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

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

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

F. Awarding restitution and damages to Plaintiff 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 Plaintiff 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**

Plaintiff demands a jury trial for all claims so triable.

Date: February 19, 2026

Respectfully submitted,

By: */s/ Ruth Sheehan*
**RHINE LAW FIRM**
Ruth Sheehan, NC Bar # 48069
Email: ras@rhinelawfirm.com
Joel R. Rhine, NC Bar # 16028
Email: jrr@rhinelawfirm.com
1612 Military Cutoff Road, Suite 300
Wilmington, North Carolina 28403
Telephone: (910) 772-9960
Fax: (910) 772-9062

Raina C. Borrelli*
**STRAUSS BORRELLI PLLC**
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com

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