IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

TYRA OMIRIN, individually, and on behalf of all others similarly situated, *Plaintiff,* v. BUMBLE INC., a Delaware corporation; and DOES 1 through 10, inclusive, *Defendant.*	Civil Action No. 1:26-cv-398 CLASS ACTION [JURY TRIAL DEMANDED]

CLASS ACTION COMPLAINT

1. Plaintiff Tyra Omirin and all others similarly situated ("Plaintiff") brings this class action against Defendant Bumble Inc. ("Bumble" or "Defendant") upon information and belief, and based on the investigation of their attorneys, for its failure to properly secure and safeguard Plaintiff's and Class Members' Personally Identifiable Information[1] stored within Defendant's information network, including without limitation, their full names, dates of birth, addresses, home and cell phone numbers, Social Security Numbers and account numbers (these types of information, *inter alia*, being thereafter referred to, collectively, as "Personally Identifiable Information" or "PII").

[1] PII generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

INTRODUCTION

2. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and other similarly situated persons in the massive and preventable cyberattack that occurred on Defendant's data servers on or around January 2026, during which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII which was being kept unprotected (the "Data Breach").

3. Plaintiff further seeks to hold Defendant responsible for not ensuring that the PII was maintained in a manner consistent with industry standards, statute and regulation.

4. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII as a requirement for the provision of services. Therefore, at all relevant times, Defendant knew or should have known that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

5. By obtaining, collecting, using and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

6. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized third party hacker—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Plaintiff and Class Members in the future

or selling their PII to another cybercriminal to do so. Plaintiff and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

7. The Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a proposed class action in which the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, the proposed Class includes more than 100 members, and minimal diversity exists because at least one Class member is a citizen of a state different from Defendant.

8. Venue is proper in this forum pursuant to 28 USC § 1391 because (1) Defendant is headquartered in the City of Austin and (2) many of the acts underlying each of the causes of action below occurred in or otherwise arose out of the City of Austin.

PLAINTIFF

9. Plaintiff Tyra Omirin is a Texas citizen and a user of Bumble's services whose PII was accessed and acquired by unauthorized third-party hackers as a result of the Data Breach.

10. Plaintiff initially provided her highly sensitive PII to Defendant in connection with the services they received. Plaintiff was required to provide her PII in order to obtain those services. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

11. At all times relevant herein, Plaintiff has been a member of the putative Class.

12. Plaintiff's PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PII. Plaintiff's PII was within the possession and control of Defendant at the time of the Data Breach.

13. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring their personal and financial accounts and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

14. 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 in and as a result of the Data Breach.

15. Plaintiff has suffered actual injury in the form of the lost benefits of her bargain with Defendant. Plaintiff entered into an agreement with and provided payment to Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect her PII. Plaintiff would not have entered into such an agreement and would not have paid Defendant the amount that she paid had she known that Defendant would not reasonably and adequately protect her PII. Plaintiff has thus suffered actual damages in an amount at least equal to the difference in value between the services that include reasonable and adequate data security that she bargained for.

16. Plaintiff has suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PII.

17. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PII being placed in the hands of unauthorized third parties/criminals.

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

DEFENDANT

19. Bumble, Inc. is a Texas stock corporation with its principal offices located at 1105 West 41st Street, Austin, Texas 78756. Bumble, Inc. may be served with Summons and Complaint through its registered agent CT Corporation System at 1999 Bryan St., Suite 900, Dallas, TX 75201.

20. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does 1 to 5 are unknown to or presently being investigated by Plaintiff at this time, and Plaintiff, therefore, sues said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as a Doe party is negligently, willfully or otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiff, as herein alleged. Plaintiff will seek leave of Court to amend this Complaint to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

21. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does 6 to 10 are unknown to or presently being investigated by Plaintiff at this time, and Plaintiff, therefore, sues said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as a Doe party negligently entrusted Plaintiff's and Class Members' PII to the other Defendants or is otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiff, as herein alleged. Plaintiff will seek leave of Court to amend this Complaint

to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

22. Doe parties were agents, servants, employees, partners, distributors, joint ventures, Business Associates of each other, and/or otherwise entrusted Defendants with Plaintiff's and Class Members' PII and that, in doing the acts herein alleged, were acting within the course and scope of said agency, employment, partnership joint venture or Business Associate relationship. Each and every aforesaid Defendant was acting as a principal and was negligent or grossly negligent in the selection, hiring, and training of each and every other Defendant, ratified the conduct of every other Defendant as an agent, servant, employee, joint venture, or Business Associate, or otherwise negligently entrusted Plaintiff's and Class Members' PII to one another.

23. Each of the Defendants was and is an agent of the other Defendants. Each Defendant, in acting or omitting to act as alleged in this Complaint, was acting in the course and scope of its actual or apparent authority pursuant to such agencies, and/or the alleged acts or omissions of each Defendant as an agent were subsequently ratified and adopted by each agent as a principal. Each Defendant, in acting or omitting to act as alleged in this Complaint, was acting through its agents, and is liable based on the acts and omissions of its agents.

24. There existed a unity of interest in ownership between all Defendants such that the individuality and separateness between them ceased where they were the alter ego of one another, in that, among other things, Defendants controlled, dominated, managed, and operated the other Defendants as their alter egos.

COMMON FACTUAL ALLEGATIONS

Defendant's Business Practices

25. Bumble is an information technology services company that operates several national and international online dating sites and is headquartered in the State of Texas. As a prerequisite to providing its services, Bumble requires its users to provide it with their sensitive PII such as financial and banking information, names, addresses, sexual orientations, along with other information. As a result, Bumble collects and stores the sensitive PII of those individuals as a part of its ordinary business practices.

26. In connection with its collection of user PII, Bumble promised its users that it would implement reasonable and adequate data security safeguards to protect that sensitive PII. To demonstrate, Bumble's public-facing Privacy Policy states the following: "Here at Bumble, we pride ourselves on taking all appropriate and reasonable security measures to: help protect your information against loss, misuse, and unauthorized access or sharing; protect the confidentiality of your personal information, such as by using secured servers with firewalls."[2] However, as evidenced below, Bumble did not adhere to those promises and instead allowed unauthorized third-party hackers to gain access to that PII.

The Cyberattack

27. On or around January 2026, the cyber-hacker group ShinyHunters executed a phishing attack on Defendant's data servers. During that Data Breach, ShinyHunters accessed, exfiltrated and acquired over 30 gigabytes of files containing PII.[3]

28. Since the data breach, ShinyHunters has released a sample of the stolen data to the dark web, which contained, *inter alia*, the following PII for a subset of Defendant's users: full

[2] https://bumble.com/privacy-policy/en#security-and-age.
[3] https://therecord.media/bumble-match-dating-apps-data-breaches.

names, dates of birth, addresses, home and cell phone numbers, Social Security Numbers, account numbers, chat history, and dating history.[4]

29. By releasing a sample of the stolen data, ShinyHunters has demonstrated that it has both reviewed the data it acquired from Defendant and that it intends to (and indeed, already has) misuse that stolen data in a manner which will and has already caused harm to Defendant's users.

Defendant Improper Storage of Class Members' PII

30. Defendant acquired, collected, stored and assured reasonable security over Plaintiff's and Class Members' PII.

31. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

32. By obtaining, collecting and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties over the PII and knew or should have known that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

33. Plaintiff and Class Members have taken reasonable steps to maintain their PII's confidentiality. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

34. Defendant could have prevented the Data Breach, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff and Class

[4] *Id.*

Members' PII.

35. Additionally, that the Data Breach was caused by a phishing attack indicates that Defendant's data security was not up to par. Phishing attacks are when scammers use email or text messages to try to steal passwords, account numbers, or Social Security numbers from users or employees of a company. If cyber criminals get that information, they will use it to access email, bank, or other accounts. Or they could sell the information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.[5]

36. Phishing attacks are rampant and hackers such as ShinyHunters target companies that collect sensitive PII through phishing attacks due to the quantity and value of the PII that they collect during the ordinary course of business.

37. Despite being common, phishing attacks are easily preventable through known prophylactic measures such as implementing organizational-wide two factor authentication or adequate employee cybersecurity training. That Defendant fell victim to a phishing attack indicates that they did not implement adequate data security to protect user PII.

38. Defendant's negligence in safeguarding Plaintiff and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

39. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated

[5] https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams#:~:text=To%20Report%20Phishing-,How%20To%20Recognize%20Phishing,from%20a%20scammer%2C%20who%20might

operation with the resources to put adequate data security protocols in place.

40. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff and Class Members' PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

41. In failing to adequately secure Plaintiff's and Class Member's sensitive data, Defendant breached duties it owed Plaintiff and Class Members under statutory and common law. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

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

43. Defendant owed a duty to Plaintiff and Class Members to design, maintain and test its computer systems, servers and networks to ensure that all PII in its possession was adequately secured and protected.

44. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

45. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

46. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

47. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust their PII to Defendant.

48. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

49. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

Value of the Stolen Sensitive Information

50. PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

51. The high value of PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank

details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[7] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[8]

52. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Equifax data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

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

54. Identity thieves can use PII, such as that of Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud,

---

6 *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the- dark-web-how-much-it-costs/

7 *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

8 *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

55. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Plaintiff's and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

56. There may be a time lag between when harm occurs versus when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

57. The harm to Plaintiff and Class Members is especially acute given the nature of the leaked data.

58. When cybercriminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

[9] *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theftand-the-value-of-your-personal-data.

59. And data breaches are preventable.[10] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n 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."[11] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[12]

60. 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*.[13]

61. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

62. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable

---

[10] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK

[11] *Id.* at 17.

[12] *Id.* at 28.

[13] *Id.*

measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this action on behalf of herself and the following class and sub-class definitions (collectively, the "Classes"):

> The "Nationwide Class":
> All individuals whose PII was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach that occurred on or around January 2026.
>
> The "Texas Sub-Class":
> All individuals residing in the State of Texas whose PII was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach that occurred on or around January 2026.

64. Excluded from each of the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

65. In the alternative, Plaintiff will request additional subclasses as necessary based on the types of PII that were compromised.

66. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

67. This action has been brought and may properly be maintained as a class action because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Plaintiff and Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using and/or safeguarding their PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Plaintiff's and Class Members' PII;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

11) Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and

12) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Predominance: Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class

Members' data was improperly stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

d. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

68. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

69. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's

policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

70. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

71. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT 1
Negligence
(On behalf of the Nationwide Class)

72. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

73. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiff's and Class Members' PII on its computer systems and networks.

74. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

75. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

76. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

77. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

78. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

79. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

80. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained thereon.

81. The Defendant had reason to anticipate the criminal act of unauthorized parties accessing the Plaintiff's and Class Members' PII, because of the widespread prior data breach attacks and theft of PII.

82. Plaintiff's and Class Members' willingness to entrust Defendant with its PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

83. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiff and/or the remaining Class Members.

84. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party

to gather Plaintiff's and Class Members' PII, misuse the PII and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

85. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent considering the foreseeable risks and known threats.

86. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

87. The law further imposes an affirmative duty on the Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

88. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members. Plaintiff's and Class Members' PII was

accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing and maintaining appropriate security measures.

89. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

90. The damages Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

91. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

92. Defendant violated 15 U.S.C. § 45 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 it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members, partly for the similar reasons alleged above in ¶¶ 29-35 and 54-56.

93. As a direct and proximate result of Defendant's negligence Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PII is used, (iii) the compromise, publication and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII, (v) lost opportunity costs associated with effort expended and the loss of productivity 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 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PII, which may 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 Plaintiff's and Class Members' PII in its continued possession, (viii) loss of benefits of their bargains in that Plaintiff and Class Members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII, thus suffering actual damages in an amount at least equal to the difference in value between the services that include reasonable and adequate data security that they bargained for, and the services that do not that they actually received, and (ix) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

94. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to shame and humiliation from their private information being disclosed to unauthorized parties, emotional distress, loss of privacy and control over their PII, lost time, annoyance, interference and inconvenience as a result of the Data Breach, anxiety over the impact of cybercriminals accessing, misusing and selling Plaintiff's PII.

95. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of

their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession.

96. Moreover, the injuries, as alleged above, that Plaintiff and Class Members have suffered and will continue to suffer are the kind of injuries that ordinarily do not occur in the absence of Defendant's negligence, including but not limited to failure to implement security measures to protect Plaintiff's and Class Members' PII, failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII, by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII; failing to adequately train its employees to not store PII longer than absolutely necessary, failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII, failing to implement processes to quickly detect data breaches, security incidents or intrusions, failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats, and, failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, denying Plaintiff and Class Members the opportunity to take meaningful, proactive steps to, inter alia, secure and/or access their PII.

97. Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII. Defendant, in turn, stored that information on Defendant's computer systems, servers, networks, and data security systems, which was within Defendant's exclusive control. Defendant's failure to adequately secure and safeguard Plaintiff's and Class Members' PII stored within the Defendant's information network invited and caused the Data Breach.

Cybercriminals regularly exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system.[14] Moreover, Defendant's failure to provide timely and clear Data breach notification to Plaintiff and Class Members, the knowledge of which was in Defendant's exclusive control, caused Plaintiff and Class Members to lose the opportunity to take meaningful, proactive steps to, inter alia, secure and/or access their PII.

98. Plaintiff and Class Members have suffered injuries and will continue to suffer injuries that were not due to any voluntary action or contribution on the part of the Plaintiff and Class Members.

99. As a direct and proximate result of Defendant's negligence Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PII is used, (iii) the compromise, publication and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII, (v) lost opportunity costs associated with effort expended and the loss of productivity 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 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PII, which may 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 Plaintiff's and Class Members' PII in its continued possession, (viii) loss of

[14] *See* Cybersecurity & Infrastructure Security Agency, Cybersecurity Advisory, "Weak Security Controls and Practices Routinely Exploited for Initial Access" (December 8, 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a

benefits of their bargains in that Plaintiff and Class Members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII, thus suffering actual damages in an amount at least equal to the difference in value between the services that include reasonable and adequate data security that they bargained for, and the services that do not that they actually received, and (ix) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

COUNT 2
Breach of Implied Contract
(On behalf of the Nationwide Class)

100. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

101. Plaintiff and Class Members provided their PII to Defendant in exchange for obtaining services, thereby entering into implied contracts with Defendant, pursuant to which Defendant agreed to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

102. Defendant solicited, offered, and invited Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining Defendant's services and as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offer, provided their PII, and paid money to Defendant.

103. As a condition of being customers of Defendant, Plaintiff and Class Members provided and entrusted their PII to Defendant. In so doing, Plaintiff and Class Members entered

into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

104. Defendant was aware of its obligations and promises to reasonably secure Plaintiff's and Class Members' PII. To demonstrate, Defendant provided a copy of its Privacy Policy to each of its users. That notice stated that "Here at Bumble, we pride ourselves on taking all appropriate and reasonable security measures to: help protect your information against loss, misuse, and unauthorized access or sharing; protect the confidentiality of your personal information, such as by using secured servers with firewalls."[15] The notice also provided, among other things, that Defendant would not disclose the Plaintiff's and Class Members' PII to anyone outside of certain, specific circumstances.

105. Defendant's data security promises and representations were incorporated within and formed a part of the implied contractual agreements between the Defendant and the Plaintiff and Class Members. In entering into agreements with Defendant, Plaintiff and Class Members reasonably believed and relied upon Defendant's Privacy Notice and any other data security representations it made. As a result, they came to reasonably expect that Defendant would take reasonable and adequate measures to protect their PII—including, *inter alia*, by complying with relevant industry standard, laws, and regulations.

106. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII while in Defendant's possession. Defendant could not provide competent services without the

[15] https://bumble.com/privacy-policy/en#security-and-age.

sensitive and confidential information, including the PII that Plaintiff and Class Members provided. Likewise, Plaintiff and Class Members would not have entrusted their PII and paid money to Defendant in the absence of Defendant's implied contract between them. Defendant's obligation under the implied agreement was to keep Plaintiff's and Class Members' PII reasonably secure.

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

108. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

109. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and noneconomic harm, including the loss of the benefits of their bargains.

COUNT 3
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

110. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

111. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

112. Plaintiff and Class Members entered into agreements with Defendant for services.

113. Plaintiff and Class Members performed all duties under their contracts with Defendant.

114. All conditions required for Defendant's performance under the contracts have occurred.

115. Incorporated in the contracts as a matter of law was the covenant of good faith and fair dealing, which prevents a contracting party from engaging in conduct that frustrates the other party's rights to the benefits of the agreement. The implied covenant imposes on a contracting party not only the duty to refrain from acting in a manner that frustrates performance of the contract, but also the duty to do everything that the contract presupposes that the contracting party will do to accomplish its purposes.

116. Here the implied covenant of good faith and fair dealing required Defendant, under the terms of the agreements, which state that Defendant will protect the Plaintiff's and Class Members' PII, to safeguard and protect from disclosure to third parties of their PII which was entrusted to Defendant only for the purposes of performing services related to the use of its dating app. Plaintiff and the Class Members could not enjoy Defendant's services without the safeguarding and protection of their PII.

117. Defendant breached the implied covenant of good faith and fair dealing by engaging in the following deliberate acts: (a) failing to implement and maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other

personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

118. Defendant acted in bad faith and/or with malicious motive in causing damages to Plaintiff and Class Members and denying them the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT 4
Unjust Enrichment
(On behalf of the Nationwide Class)

119. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein. This cause of action is brought in the alternative to Plaintiff's and Class Members' claims under law.

120. By their wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

121. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PII to Defendant for the purpose of purchasing services from Defendant, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PII secure.

122. Defendant was aware, or should have been aware, that reasonable consumers would have wanted their PII kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were substandard for that purpose.

123. Defendant was also aware that if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to engage with Defendant.

124. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to

make purchases, engage in commerce therewith, and seek services or information. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to make a rational and informed purchasing decision and took undue advantage of Plaintiff and Class Members.

125. Defendant was unjustly enriched at the expense of Plaintiff and Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members. By contrast, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

126. Since Defendant's profits, benefits, and other compensation were obtained by improper means, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

127. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from their wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

COUNT 5
Violations of the Texas Deceptive Trade Practices Act ("DTPA")
Texas Business & Commerce Code §17.50, *et seq.*
(On behalf of the Texas Sub-Class)

128. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

129. Defendant was a supplier of "services" and engaged in "trade" and "commerce" with Plaintiff and Sub-Class Members because they engaged in the advertisement and sale of goods and services to Plaintiff and Sub-Class Members for personal, family or household purposes. Texas Business & Commerce Code §17.45.

130. In connection with those consumer transactions, Defendant engaged in the following conduct prohibited by the DTPA:

a. "Intentionally" misrepresenting that goods and services have certain quantities, characteristics, ingredients, uses, or benefits (Texas Business & Commerce Code § 17.46(b));

b. "Intentionally" misrepresenting that goods or services are of a particular standard, quality, grade, style or model (Texas Business & Commerce Code § 17.46(b));

c. "Intentionally" advertising goods or services with the intent to not sell them as advertised. (Texas Business & Commerce Code § 17.46(b)).

131. During all relevant times, Defendant thereby violated the DTPA by selling services that they promised and represented would include reasonable and adequate data security safeguards for the PII that they collected in connection with those services but which did not include such safeguards. Defendant knowingly and intentionally engaged in the acts and practices described herein in violation of the DTPA.

132. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Sub-Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and noneconomic harm, including the loss of the benefits of their bargains.

133. Under Texas Business & Commerce Code §17.50, Plaintiff and Sub-Class Members are each entitled to recover their economic damages, damages for mental anguish as found by a trier of fact, attorneys' fees, costs and prejudgment interest.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own behalf and on behalf of each member of the proposed Class, respectfully request that the Court enter judgment in favor of Plaintiff and the Class and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class and Sub-Class, including appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, statutory, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief, pursuant to Plaintiff's and Class Members' claims for Negligence, Breach of implied Contract and Breach of the Implied Covenant of Good Faith and Fair Dealing. While Plaintiff's and Class Members' PII remains in Defendant's inadequately protected computer systems and networks, their PII remains exposed and vulnerable to imminent unauthorized access by more cybercriminals. Therefore, there is an inadequate remedy at law

because Plaintiff and Class Members are forced to permit their PII be subject to an ongoing risk and seek redress after another cyber-attack. This is especially true because identity theft results in years of constant surveillance of financial and personal records, monitoring, and loss of rights that money damages are unable to fully rectify. Thus, Plaintiff and Class Members make a request including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

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

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

c. requiring Defendant to delete and purge Plaintiff's and Class Members' PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

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

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

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

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

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

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

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law; and

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: February 19, 2026

By: /s/ Craig D. Cherry

CRAIG D. CHERRY
State Bar No. 24012419
TANNER R. DANIELS
State Bar No. 24143614
CHERRY JOHNSON SIEGMUND JAMES PC
7901 Fish Pond Rd., 2nd Floor
Waco, TX 76710
Phone: 254-732-2242
Fax: 866-627-3509

Thiago M. Coelho (CA S.B. # 324715)*
WILSHIRE LAW FIRM, PLC
660 S. Figueroa St., Sky Lobby
Los Angeles, California 90017
Telephone: (213) 381-9988
Email: Thiago.coelho@wilshirelawfirm.com
**Pro Hac Vice* admission forthcoming

Attorneys for Plaintiff and the Class

ClassAction.org
