Michael F. Ram (SBN 104805)
Marie N. Appel (SBN 187483)
Jean Martin (*To Be Admitted Pro Hac Vice*)
Francesca Kester Burne (*To Be Admitted Pro Hac Vice*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
Email: mram@forthepeople.com
mappel@forthepeople.com
jeanmartin@forthepeople.com

Samuel J. Strauss (*To Be Admitted Pro Hac Vice*)
Raina Borelli (*To Be Admitted Pro Hac Vice*)
Brittany Resch (*To Be Admitted Pro Hac Vice*)
TURKE & STRAUSS LLP
613 Williamson Street, Ste. 201
Madison, WI 53703
Telephone: (608) 237-1775
Email: sam@turkestrausss.com
raina@turkestrauss.com
bittanyr@turkestrauss.com
Attorneys for Plaintiff

THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA

YOLANDA BRADFORD, *individually and on behalf of all others similarly situated,*

Plaintiff,

v.

HATCH BANK

Defendant.

Case No.: '23CV0465 JM BLM

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff, Yolanda Bradford, through her attorneys, brings this Class Action Complaint against the Defendant, Hatch Bank, ("Hatch" or "Defendant"), and alleges as follows:

INTRODUCTION

1. Between January 30 and January 31, 2023, Hatch, a company that provides online banking services to other financial technology companies, lost control over thousands of consumers' names and Social Security numbers during a two-day data breach by cybercriminals ("Data Breach").

2. Hatch's breach differs from typical data breaches because it affects consumers who had no relationship with Hatch, never sought one, and never consented to Hatch collecting and storing their information.

3. Hatch sourced their information from third parties, stored it on Hatch's systems, and assumed a duty to protect it, advertising that Hatch "understands that the security of your personal and account information is important to you." But Hatch never implemented the security safeguards needed despite acknowledging its importance.

4. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the personal information and PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's

personally identifying information ("PII")—rendering them easy targets for cybercriminals.

5. On information and belief, the Data Breach affected tens of thousands of consumers.

6. The information compromised in the Data Breach includes consumers' PII, including their names and Social Security numbers.

7. Plaintiff is a Data Breach victim who had no relationship with Hatch but received its breach notice in February 2023, informing her that her name and Social Security number were compromised in the Data Breach. She brings this Class Action on behalf of herself, and all others harmed by Hatch's misconduct in causing its January 2023 Data Breach.

8. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

9. Plaintiff, Yolanda Bradford, is a natural person and citizen of Texas, residing in Houston, Texas, where she intends to remain.

10. Defendant, Hatch Bank, is a California Corporation with its principal place of business at 1001 W. San Marcos Blvd Ste 125 San Marcos, CA 92078.

JURISDICTION & VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff and Defendant are citizens of different states.

12. Hatch is incorporated in California and maintains its principal place of business in California at 1001 W. San Marcos Blvd Ste 125 San Marcos, CA 92078. Hatch is thus a California citizen.

13. This Court has personal jurisdiction over Hatch because it is a citizen in this District and maintains its headquarters and principal place of business in this District.

14.Venue is proper because Hatch maintains its headquarters and principal place of business in this District.

BACKGROUND FACTS

Hatch

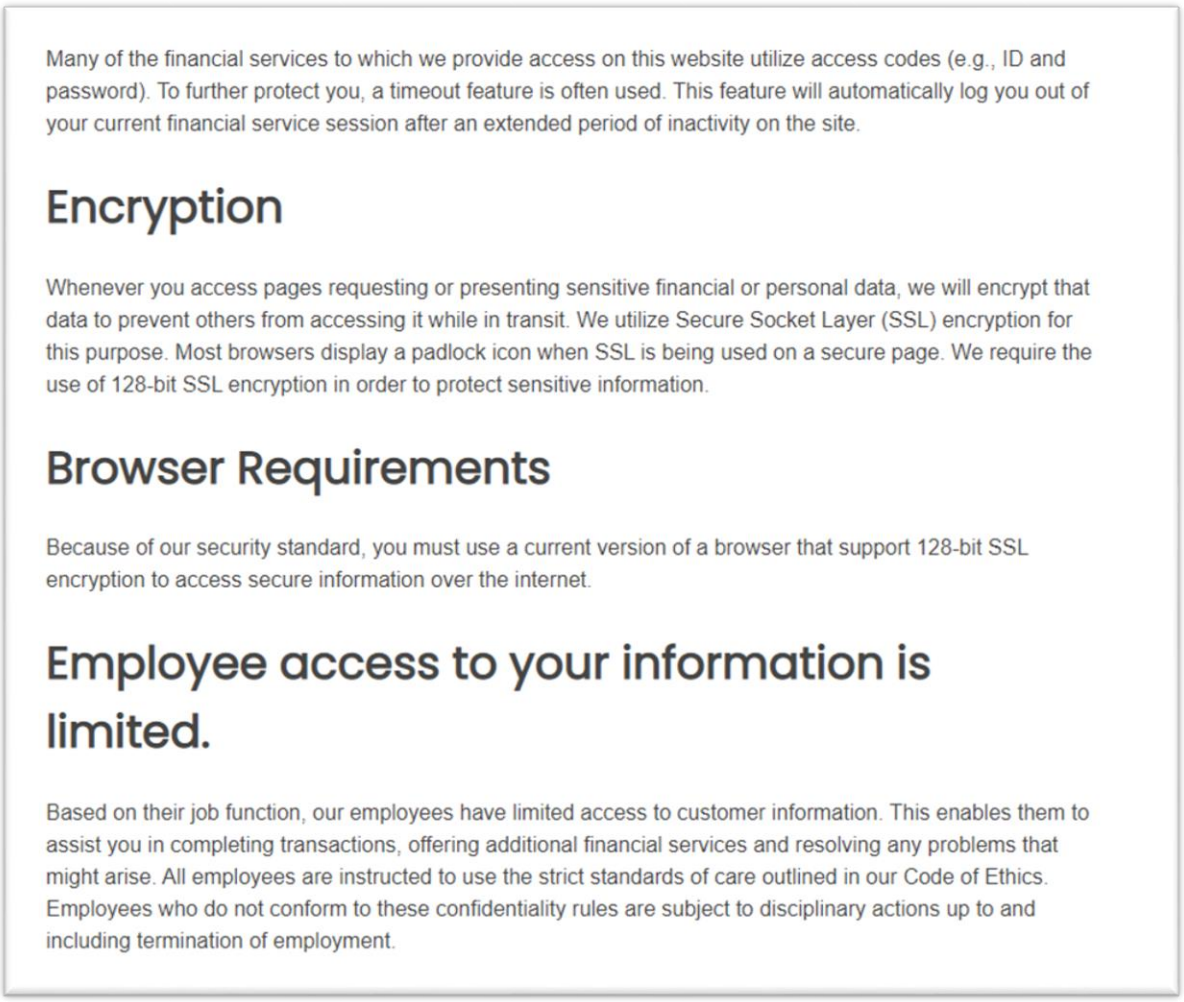
15. Hatch is a digital bank that provides online banking services to other financial technology companies.

16. As an online company dealing in highly sensitive information, Hatch should understand its duties to safeguard personal information.

17. Indeed, Hatch claims in its privacy policy that it "highly value[s] our

customers' privacy. [Hatch] has protected [the consumers'] confidential information in many ways over the years and will continue to do so."[1]

18. Additionally, Hatch advertises itself as a "leading financial institution" that secures PII through multiple features:



Many of the financial services to which we provide access on this website utilize access codes (e.g., ID and password). To further protect you, a timeout feature is often used. This feature will automatically log you out of your current financial service session after an extended period of inactivity on the site.

Encryption

Whenever you access pages requesting or presenting sensitive financial or personal data, we will encrypt that data to prevent others from accessing it while in transit. We utilize Secure Socket Layer (SSL) encryption for this purpose. Most browsers display a padlock icon when SSL is being used on a secure page. We require the use of 128-bit SSL encryption in order to protect sensitive information.

Browser Requirements

Because of our security standard, you must use a current version of a browser that support 128-bit SSL encryption to access secure information over the internet.

Employee access to your information is limited.

Based on their job function, our employees have limited access to customer information. This enables them to assist you in completing transactions, offering additional financial services and resolving any problems that might arise. All employees are instructed to use the strict standards of care outlined in our Code of Ethics. Employees who do not conform to these confidentiality rules are subject to disciplinary actions up to and including termination of employment.

19. Yet, upon information and belief, Hatch did not implement those security measures as advertised, nor were they reasonably sufficient to protect the highly

[1] Privacy Policy, Hatch Bank, https://hatchbank.com/privacy-policy/ (last visited March 6, 2023).

sensitive data Hatch collected.

20. As Plaintiff alleges above, Hatch collects data on individuals who have no relationship with it, do not want one, and have never consented to its services.

21. It does so by sourcing that information from third parties. Plaintiff's information was "received by Hatch Bank in connection with a loan [Plaintiff] applied for through Wisetack, Inc.. Hatch Bank either reviewed your application to issue a credit decision or is the owner of your current loan or credit card account issued through your relationship with Wisetack, Inc.." *See* attached **Exhibit A** for Hatch's Breach Notice.

22. Under state and federal law, businesses like Defendant have duties to protect consumers' PII and to notify them promptly about breaches.

Hatch Fails to Safeguard Consumer PII

23. Upon information and belief, a vulnerability in Hatch's internal file transfer system was first discovered by the company on January 29, 2023.[2]

24. On January 30 and January 31, 2023, hackers were first discovered to have exploited the vulnerability to steal 13,300 consumers' driver's license numbers.

[2] Hatch Bank Data Breach, TechCrunch, https://techcrunch.com/2023/03/02/hatch-bank-breach-fortra-goanywhere-exploit/#:~:text=Hatch%20Bank%2C%20a%20digital%2Dfirst,of%20customer%20Social%20Security%20numbers

25. Hatch failed to detect the hack. The supplier of Hatch's internal file sharing system had to inform Hatch of the Data Breach on February 3, 2023. *See* attached **Exhibit A**.

26. Upon information and belief, the notorious Clop ransomware gang was responsible for the cyberattack.[3] Clop is one of the most active ransomware actors, having breached over 130 organizations. [4] Hatch, an online banking company providing digital services to other financial technology company, knew or should have known of the tactics that groups like Clop employ.

27. Indeed, healthcare giant, Community Health Systems of Tennessee had been breached by Clop through the same internal file transfer vulnerability, just a month prior. [5]

28. Upon information and belief, Clop ransomware gang knew of Hatch's

---

[3] Hatch Bank Breach, TechRadar, https://www.techradar.com/news/hatch-bank-says-140000-customers-had-data-stolen-after-breach (last visited March 7, 2023).

[4] Hatch Bank Data Breach, TechRadar Pro, https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/#:~:text=The%20Clop%20ransomware%20gang%20claims,data%20from%20over%20130%20organizations. (last visited March 7, 2023).

[5] Hatch Bank discloses Data Breach, Bleeping Computer, https://www.bleepingcomputer.com/news/security/hatch-bank-discloses-data-breach-after-goanywhere-mft-hack/ (last visited March 7, 2023).

system vulnerability prior to January 29, 2023, [6] and had been exploiting it before it was discovered by Hatch or the agents, contractors, vendors, and suppliers Hatch supervised.

29. Plaintiff Yolanda Bradford is a Data Breach victim. She has no relationship with Hatch, never sought one, and never consented to the company using or storing her PII.

30. Even though Plaintiff never had a relationship with Hatch, Defendant still collected her PII and stored it in Hatch's computer systems.

31. In collecting and maintaining her and the Class's PII, Hatch assumed a duty to safeguard it according to its internal policies and state and federal law.

32. On information and belief, Hatch failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII through a security vulnerability. Hatch's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing Plaintiff's and the Class's PII. Further, Hatch's Data Breach make clear that Hatch cannot, or will not, protect the PII it retrieves and possesses on consumers.

33. Indeed, even Hatch recognizes the threat its Data Breach poses in its

[6] Clop Ransomware Breaches, https://www.cpomagazine.com/cyber-security/clop-ransomware-breaches-130-organizations-steals-1-million-chs-healthcare-patients-records/ (last visited March 7, 2023).

breach notice. It offered breach victims 12 months of credit monitoring and "encouraged" them to guard themselves and remain vigilant to "potential incidents of identity theft and fraud", offering these suggestions as ways "on what you can do to better protect against possible misuse of your information." Hatch's warning is ironic since the risk of possible misuse it warns against stems from Hatch's own inability to protect the PII it retrieves and processes of consumers, rather than the fault of the consumers.

Plaintiff's Experience and Injuries

34. Plaintiff, Yolanda Bradford, was injured by Defendant's Data Breach.

35. Despite never forming or seeking a relationship with Hatch, Plaintiff's PII was compromised in Hatch's Data Breach, compromising her Social Security number and exposing her to identity theft and fraud.

36. In fact, on December 19, 2022, a fraudulent credit card application was approved in Plaintiff's name for a Harley Davidson credit card. A month later, on January 28, 2023, Plaintiff experienced a fraudulent online purchase from Walmart. Finally, on February 28, 2023, Plaintiff was notified of yet another fraudulent attempt, this time to create an Ulta Beauty Credit card from Comenity bank. These multiple fraud attempts demonstrate that Plaintiff's information stolen in the Data Breach has been placed in the hands of cybercriminals.

37. Plaintiff has also experienced an increase in spam texts and phone calls since the Data Breach, further suggesting that her information has been placed in

the hands of cybercriminals.

38. Plaintiff does not recall ever learning that her information was compromised in a data breach incident, other than the breach at issue in this case.

39. Plaintiff suffered actual injury from the exposure of her PII —which violates her rights to privacy.

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

41. As a result of the Data Breach and the recommendations of Defendant's Notice, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring her credit information as suggested by Defendant.

42. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

43. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach.

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

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

45. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

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

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

e. Lost opportunity costs and lost wages associated with the time and

effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

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

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

49. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly

profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

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

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

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

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

54. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

55. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's 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.

Defendant failed to adhere to FTC guidelines.

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

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should: protect the personal customer information that they keep;

properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

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

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

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

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

CLASS ACTION ALLEGATIONS

62. Plaintiff is suing on behalf of herself and the proposed Class ("Class"), defined as follows:

> **All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Hatch in February 2023.**

63. Excluded from the Class is 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.

64. Plaintiff reserves the right to amend the class definition.

65. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

66. **Numerosity**. Plaintiff's claim is representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

67. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

68. **Typicality**. Plaintiff's claim is typical of Class member's 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.

69. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interest does not conflict with Class members' interests, and

Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

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

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

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

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

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

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

f. Whether Defendant's Breach Notice was reasonable;

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

h. What the proper damages measure is; and

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

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

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

72. Plaintiff realleges all previous paragraphs as if fully set forth below.

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

74. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and

providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

75. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

76. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's personal information and PII.

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

78. 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 members of the Class and the importance of exercising reasonable care in handling it.

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

80. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by

Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

81. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

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

83. 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 consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

84. 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.

85. 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.

86. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

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

88. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

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

90. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its 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.

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

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

92. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

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

94. Defendant owed a duty to Plaintiff and the Class to keep their PII confidential.

95. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and the Class's PII is highly offensive to a reasonable person. Defendant's reckless and negligent failure to protect Plaintiff's and the Class's PII

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.

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

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

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

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

100. 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.

101. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality

of Plaintiff's and Class Members' PII.

102. Plaintiff, on behalf of herself and Class Members, 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.

Count IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

103. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

104. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

105. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

106. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the

goods and services that were the subject of the transaction and have their PII protected with adequate data security.

107. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

108. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant, either directly or through their own financial institutions that used Defendant's services, as part of Defendant rendering online banking related services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

109. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiff and the Class 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.

110. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security

measures that are mandated by industry standards.

111. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

112. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant either directly or through their own financial institutions.

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

114. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) 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 identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) 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 the Class.

115. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

116. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT V:
Violations of the Unfair Competition Law,
BUS. & PROF. CODE § 17200, *et seq.*
(On behalf of Plaintiff and the Class)

117. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

118. The California Unfair Competition Law provides that:

> "[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." (BUS. & PROF. CODE § 17200.)

119. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry

standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure and prevented the loss or misuse of that PII.

120. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

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

122. Defendant's conduct was unlawful, in that it violated the policy set forth in California's Consumer Records Act, requiring the safeguard of personal information like Social Security numbers, the FTCA, as identified above, and Defendant's common law duty to safeguard PII.

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

124. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the

intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

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

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

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

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

COUNT VI
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Class)

129. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

130. 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. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

131. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges that Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

132. Pursuant to 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 employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' PII; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Classes.

133. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its customers' (i.e. Plaintiff's and the Classes') data.

134. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have 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 to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

135. The hardship to Plaintiff and the Class, if an injunction does not issue, exceeds the hardship to Defendant if an injunction is issued.

136. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. For an Order certifying the Class, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order;

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

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for

the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

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

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

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

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

monitoring;

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

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

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

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

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

xiv. 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;

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

xvi. 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; and

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2

attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues triable by a jury.

DATED this 14th day of March 2023.

By /s/ Michael F. Ram

Michael F. Ram (SBN 104805)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@forthepeople.com

Jean S. Martin*
Francesca Kester Burne*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jeanmartin@forthepeople.com
fkester@forthepeople.com

Samuel J. Strauss *
Raina Borelli *
Brittany Resch*
TURKE & STRAUSS LLP
613 Williamson Street, Ste. 201
Madison, WI 53703
Telephone: (608) 237-1775
Email: sam@turkestrausss.com
raina@turkestrauss.com
brittanyr@turkestrauss.com

Counsel for Plaintiff and the Putative Class

*Motions for *pro hac vice* admission to be filed

ClassAction.org
