Exhibit A

UNITED STATES DISTRICT COURT FOR THE

WESTERN DISTRICT OF TEXAS

AUSTIN DIVISION

Connie Yuan on behalf of herself and all others similarly situated,	§	
***Plaintiffs*,**	§	
	§	**Case No.: 1:22-cv-01355**
v.	§	
	§	
HomeTrust Mortgage, Co.,	§	
	§	
***Defendant*.**	§	

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT

Plaintiff Connie Yuan ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant HomeTrust Mortgage, Co., (hereinafter known as "HomeTrust" or "Defendant"), a Texas corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant.

Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of counsel, and facts that are a matter of public record.

I. INTRODUCTION

1. Applicants for a home mortgage loan must turn over valuable personal identifying information, including Social Security numbers, bank account information, driver's license numbers, and addresses. If stolen, this highly sensitive information can be used by identity thieves to fraudulently open new accounts, access existing accounts, perpetuate identify fraud or impersonate victims in a myriad of schemes, all of which can cause grievous financial harm, negatively impact the victim's credit score for years, and cause victims to spend hours mitigating the impact.

2. Every year, millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers' data.

3. Defendant HomeTrust, an originator and provider of residential mortgage loans, is among those companies that have failed to meet their obligation to protect the sensitive personal identifying information ("PII") entrusted to them by their customers.

4. On or around July 15, 2022, HomeTrust became aware that there was suspicious activity within its computer system.

5. From July 15, 2022, until September 27, 2022, HomeTrust engaged third parties to assist in the investigation this "suspicious activity."

6. Finally, after months of investigation, on September 27, 2022, HomeTrust determined that not only was the company was the victim of a Ransomware attacker, and but there had been unauthorized access to the network.

7. This ransomware attacker gained unauthorized access to electronic data stored by HomeTrust, including customer PII, and removed data stored by HomeTrust, including PII. The stolen PII included, but is not limited to, first and last names, Social Security numbers, and addresses (hereafter referred to as the "Data Breach").

8. As a corporation doing business in Texas, HomeTrust is legally required to secure the PII it collects by implementing reasonable and appropriate data security safeguards and protecting PII from unauthorized access.

9. As a result of HomeTrust's failure to provide adequate data security, Plaintiff's and the Class members' PII has been exposed to those who should not have access to it. Plaintiff and the Class have suffered the damages alleged below and are now at much higher risk of identity

theft and cybercrimes of all kinds.

10. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown third party or precisely what specific type of information was accessed.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing expanded credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

II. PARTIES

a. Plaintiff

15. Plaintiff Connie Yuan is a natural person, resident, and a citizen of the State of Texas, residing in Travis County.

16. On or around November 2020, Plaintiff Connie Yuan provided her PII to Defendant

HomeTrust to obtain a home mortgage loan.

17. On or around December of 2022, Plaintiff Connie Yuan received notice from HomeTrust that her PII had been accessed in the July 2022 Data Breach.

18. Because Defendant HomeTrust obtained and continues to maintain Plaintiff's PII, Defendant owed her a legal duty and obligation to protect that PII from unauthorized access and disclosure.

19. Plaintiff Connie Yuan would not have entrusted her PII to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

b. Defendant HomeTrust Mortgage, Co.

20. Defendant HomeTrust Mortgage Co. is a Texas corporation with its business headquarters in Texas and does business throughout the state of Texas as well as other multiple states.

III. JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) in that (1) this action is a class action with more than one hundred (100) Class Members; (2) Defendant is a Texas Corporation and is a citizen of Texas; (3) Plaintiff and members of the Class are citizens of the United States, and members of the Class consists of citizens of Alabama, Colorado, Florida, Georgia, New Mexico, Oklahoma, Montana and Tennessee, thus satisfying the minimal diversity requirement of 28 U.S.C. § 1332(d)(2)(A); and (4) the matter in controversy exceeds the sum or value of $1,000,000 exclusive of interests and costs.

22. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because Plaintiff

resides in the Austin Division of the Western District of Texas and a substantial part of the events or omissions giving rise to the claim occurred in the Austin Division of the Western District of Texas.

IV. FACTUAL ALLEGATIONS

a. HomeTrust's Business Operations

23. Founded in 1986, HomeTrust is a non-depository mortgage bank which services customers in Texas, as well as nationwide in at least Alabama, Colorado, Florida, Georgia, New Mexico, Oklahoma, Montana and Tennessee.

24. HomeTrust employs over 100 people and generates approximately over $23 million in annual revenue.

i. HomeTrust's Business Activities Collect and Store its Customers' PII

25. As part of the mortgage application process, HomeTrust requires customers to provide a slew of information and documentation, including copies of a valid driver's license, copies of 30-days' worth of pay-stubs, copies of W-2 forms for the last two years, copies of tax returns, copies of divorce decrees, information related to stocks and bonds, and account numbers for all credit liabilities. [1]

26. HomeTrust claims that it in order to protect their customers' personal information from unauthorized access and use, it uses "security measures that comply with Federal Law." [2] It further states that "[t]hese measures include computer safeguards and secured files and buildings."

b. Defendant Experienced a Cyberattack and Failed to Adequately Protect Plaintiffs' PII

27. On or around July 15, 2022, HomeTrust became aware that there was suspicious

[1] *See* https://www.hometrust.com/mortgage-basics/application-checklist/ (last accessed December 19, 2022).
[2] *See* https://www.hometrust.com/privacy-policy/ (last accessed December 19, 2022).

activity within its computer system. From July 15, 2022 until September 27, 2022, HomeTrust engaged third parties to "assist" in the investigation this "suspicious activity." Finally, after months of so-called investigation, on September 27, 2022, HomeTrust determined that not only was the company was the victim of a Ransomware attacker, and but there had been unauthorized access to the network.

28. This ransomware attacker gained unauthorized access to electronic data stored by HomeTrust, including customer PII, and removed data stored by HomeTrust, including PII. The stolen PII included, but is not limited to, first and last names, Social Security numbers, and addresses (hereafter referred to as the "Data Breach").

29. On November 23, 2022, HomeTrust provided notice of the Data Breach to the Texas Attorney General's Office, estimating that the total number of impacted persons was 12,899 people.

30. This was followed by a notice[3] of the Data Breach to the impacted customers, advising these people that an "unauthorized individual" and gained access to the network and had "removed some data" from the system, including the PII of the impacted customers.

31. The notice went on to advise these impacted customers to "remain vigilant" and review "account statements and credit reports closely." [4]

32. HomeTrust also agreed to provide "identity protection services" through a third-party vendor named IDX. [5]

c. <u>The PII exposed by HomeTrust as a Result of it Inadequate Data Security is Highly Valuable on the Black Market.</u>

[3] *See* https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-724.pdf (last accessed December 20, 2022).
[4] *Id.*
[5] *Id.*

33. The information exposed by HomeTrust is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

34. This exposure is tremendously problematic. Cybercrime is rising at an exponential rate.

35. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

36. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

37. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay 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 $4 to $1000 dollars on the dark web. [6]

38. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social

[6] https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=19fded6213f1 (last accessed December 19, 2022)

Security number and assuming your identity can cause a lot of problems.[7]

39. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

40. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

41. Because of this, the information compromised in the Data Breach here is significantly more valuable than the loss of, for example, credit card information in a retailer data breach. While in that case victims can cancel or close credit and debit card accounts, for those who had their data disclosed in the instant Data Breach, it is impossible to "close" and difficult, if not impossible, to change Social Security number, driver's license number, bank information, passport number, name, date of birth, and addresses.

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

43. In 2021, a record 1,862 data breaches occurred, resulting in approximately

[7] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 19, 2022).
[8] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers- has-millionsworrying-about-identity-theft (last accessed December 19, 2022).

293,927,708 sensitive records being exposed, a 68% increase from 2020.[9]

44. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

45. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market." [11]

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

47. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and Class members that their PII had been stolen. It took Defendant almost five months to notify them.

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

---

[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[10] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed December 19, 2022).
[11] https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html#:~:text=%E2%80%9CCompared%20to%20credit%20card%20information,Walter%2C%20senior%20director%20at%20RedSeal. (last accessed December 19, 2022).

opened accounts or misuse of existing accounts.

49. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

50. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[12]

51. The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[13]

d. HomeTrust Failed to Comply with Federal and Texas State Regulations Related to Data Protection

52. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions.

53. For example Defendants are required the Texas Identity Theft Enforcement and Protection Act and various other laws and regulations to protect Plaintiff's and Class members' Medical Information and to handle notification of any breach in accordance with applicable

[12] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last accessed December 19, 2022).
[13] *Id.*

breach notification statutes. Indeed, as part of the Texas Identity Theft Enforcement and Protection Act, FMC was required to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."

54. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

55. 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. Among other things, the guidelines note businesses should 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. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. [15]

56. Additionally, the FTC recommends that companies 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. [16]

[14] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed December 19, 2022).
[15] *Id.*
[16] *Id.*

57. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. [17]

58. By allowing an unknown third party to access HomeTrust's data storage system and expose customers' PII, HomeTrust failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data, and as a result, allowed an unknown third party to access its data storage system and expose customers' PII. HomeTrust's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. In addition, the Gramm-Leach-Bliley Act ("GLBA"), provides "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a). Defendant is a financial institution under the GLBA.

60. The GLBA also commands various agencies to craft standards for data security for financial institutions such as Defendant. 15 U.S.C. § 6801(b)(2). Those standards are set forth in 16 C.F.R. § 314, et seq. In particular, those standards require financial institutions to "develop, implement, and maintain a comprehensive information security program that is

[17] https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last accessed December 19, 2022).

written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue." 16 C.F.R. § 314.3.

61. Among other specific requirements, 16 C.F.R. § 314.4 required Defendant to: (a) designate an employee or employees to coordinate your information security program; (b) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks; (c) design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (d) oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and requiring your service providers by contract to implement and maintain such safeguards; and (e) evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

62. Defendant failed to fulfill those requirements as mandated under the GLBA and the subsequent regulations enacted pursuant to it, resulting in the Data Breach and the damages to Plaintiffs and the Class members.

e. HomeTrust Failed to Comply with Industry Standards Related to Data Protection

63. Several best practices have been identified that at a minimum should be

implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

65. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

66. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

f. HomeTrust Breached its Duties to its Customers

67. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of

data breaches;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

68. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks, Defendant negligently and unlawfully failed to safeguard Plaintiff' and Class Members' PII by allowing cyberthieves to access Defendant's IT systems and remove data which contained unsecured and unencrypted PII.

69. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

g. Plaintiff Engaged in Measures to Attempt to Secure Their PII After the Breach

70. Plaintiff Yuan is a customer of HomeTrust, having obtained a mortgage with Defendant in November 2020.

71. As a condition of applying for and obtaining that mortgage, Plaintiff Yuan was required to provide HomeTrust with her PII. She did so with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Had she known that HomeTrust would not take reasonable steps to protect her PII, she would not have provided it to HomeTrust or paid mortgage fees or mortgage interest to HomeTrust in the amount she did. Plaintiff Yan reasonably believed that the money she paid to HomeTrust would be used to provide reasonable data security for her pII.

72. Upon receiving notice of the Data Breach some time in December of 2022, Plaintiff Yuan researched her options to respond to the theft of her name and Social Security Number. Plaintiff Yuan spent and will continue to spend additional time reviewing her financial accounts for fraudulent activity. This is time Plaintiff Yuan otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

73. Plaintiff Yuan suffered actual injury from having her PII exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of her PII—a form of intangible property that Plaintiff Yuan entrusted to HomeTrust as a condition of applying for and receiving a home loan; (b) loss of her privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

74. As a result of the Data Breach, Plaintiff Yuan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. In addition, Plaintiff Yuan will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

h. Plaintiff and the Class Suffered Damages

75. HomeTrust had obligations created by contract law, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

76. The ramifications of Defendant's failure to keep customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

77. The PII belonging to Plaintiffs and Class members is private, sensitive in nature, and was inadequately protected by Defendant who did not obtain Plaintiffs' or Class members' consent to disclose such PII to any other person as required by applicable law and industry standards.

78. The Data Breach was a direct and proximate result of HomeTrust's failure to: (a) properly safeguard and protect Plaintiffs' and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII; and protect against reasonably foreseeable threats to the security or integrity of such information.

79. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customers' PII.

80. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions

into its systems and, ultimately, the theft of PII.

81. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

82. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims.[18]

83. As a result of the Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;
b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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;
d. 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 appropriate measures to protect the PII in its possession; and
e. Current and future costs in terms of time, effort, and money that will be

[18] https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf (last accessed December 19, 2022).

expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

84. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

85. To date, other than providing 1 year of identity monitoring services, Defendant does not appear to be taking any measures to assist Plaintiffs and Class members

86. Defendant's offer of 1 year of identity monitoring services is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.

i. **HomeTrust's Delay in Identifying and Reporting the Breach Caused Additional Harm**

87. Although their PII was improperly exposed in or about July of 2022, Plaintiffs and the Class were not notified of the Data Breach until give months later, on or about December of 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

88. As a result of HomeTrust's delay in detecting and notifying customers of the Data Breach, the risk of fraud has been driven even higher.

V. CLASS ACTION ALLEGATIONS

89. Plaintiff brings this Action on behalf of herself and all other persons similarly situated.

90. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **Nationwide Class:** *All persons whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in December 2022 (the "Class").*
>
> **Texas Subclass:** *All persons from Texas whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in December 2022 (the "Texas Subclass").*

91. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

92. Plaintiff hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 42(a), (b)(2), and (b)(3).

93. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable.

94. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' 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's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

95. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

96. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

98. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action

as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

99. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

100. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

101. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

FIRST COUNT - NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

102. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

103. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain a home mortgage.

104. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

105. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein,

and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

106. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

107. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

109. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiff's and Class Members' PII;

e. Failing to detect in a timely manner that Plaintiff's and Class Members' PII had been compromised; and

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

110. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

111. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to Class Members.

112. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

113. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and unsecure manner.

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT - BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and All Class Members)

115. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

116. When Plaintiff and Class Members provided their PII to Defendant in exchange for a home mortgage, they entered into implied contracts and they did so with the belief that Defendant had agreed to reasonably protect such information.

117. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

118. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

119. Plaintiff and Class Members provided labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so. Class Members similarly paid money to Defendant for its services with the reasonable belief and expectation that Defendant would use part of that payment to obtain adequate data security for the PII consumers entrusted to Defendant. Defendant failed to do so.

120. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

121. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

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

123. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

124. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

125. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

126. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT - NEGLIGENCE PER SE
(On Behalf of Plaintiff and All Class Members)

127. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

128. Pursuant to the Federal Trade Commission 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 Class Members' PII.

129. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

130. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

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

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

133. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH COUNT - BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

134. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

135. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act

primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

136. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them, in particular, to keep secure their PII.

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

138. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

139. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

140. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

141. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (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; (v) the continued risk to 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 the PII in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

142. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT - INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

143. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

144. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts§ 652B (1977).

145. Plaintiff and Class Members had a reasonable expectation of privacy in the PII that Defendant mishandled.

146. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

147. By intentionally failing to keep Plaintiff's and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

148. Defendant knew that an ordinary person in Plaintiff or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

149. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

150. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class Members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

151. The conduct described above was at or directed at Plaintiff and the Class Members.

152. As a proximate result of such intentional misuse and disclosures, Plaintiff and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

153. In failing to protect Plaintiff's and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

SIXTH COUNT - UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

154. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

155. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count, the second count listed in this Complaint.

156. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including money it earns through work performed by

Plaintiff and the Class Members and money paid to it by consumers in exchange for its services.

157. 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.

158. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they performed work for and Defendant and on Defendant's behalf and in so doing provided Defendant with their PII. Class members also conferred a monetary benefit in the form of payments to Defendant for its services and also entrusted Defendant with their PII In exchange, Plaintiff and Class Members should have received from Defendant compensation in the form of adequate data security designed to safeguard their PII.

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

160. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

161. 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 use that money to implement appropriate data management and security measures that are mandated by industry standards.

162. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

163. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

164. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

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

166. 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: (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to 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 their continued possession; and (g) 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.

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

168. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they 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.

VII. JURY TRIAL DEMANDED

169. Plaintiff demands a trial by jury on all claims so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her 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 Class Members, 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 Class Members;

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

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

vi. 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;

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

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

ix. 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;

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

xi. 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 Class Members;

xii. 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;

xiii. 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;

xiv. 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;

xv. 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;

xvi. 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, and consequential 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.

DATED: December 22, 2022

Respectfully submitted,

s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Samuel J. Strauss*
Raina C. Borrelli*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

Matthew R. Wilson
MEYER WILSON CO., LPA
305 W. Nationwide Blvd
Columbus, OH 43215
Tel. (614) 224-6000
Fax. (614) 224-6066
mwilson@meyerwilson.com

Layne C. Hilton
MEYER WILSON CO., LPA
900 Camp Street, Suite 337
New Orleans, LA 70130
Tel. (614) 224-6000
Fax. (614) 224-6066
lhilton@meyerwil.com

ATTORNEYS FOR PLAINTIFFS

***Pro Hac Vice Forthcoming**