THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

SAVANNAH KOLSTEDT, et al., *individually and on behalf of all others similarly situated,* Plaintiffs, v. TMX FINANCE CORPORATE SERVICES, INC.; TMX FINANCE LLC d/b/a "TitleMax" d/b/a "TitleBucks" d/b/a "InstaLoan," Defendants.	Civil Action No. 4:23-cv-00076-RSB-CLR **JURY TRIAL DEMANDED**

CONSOLIDATED COMPLAINT – CLASS ACTION

Plaintiffs Sonya Albert, Makecia Berry, Ryan Carder, Sheneequa Carrington, Lana Clark, Victoria Coria, Antonio DeJesus, Leon Diaz, Tommy Domino, Patsy Eslinger, Evelyn Francis, Jeremiah Gills, Melvin Nicholas , Dewayne Jackson, Yolanda Jackson, Adrian Johnson, Chaplin Johnson, Von King, Ebony Millner, Lakendra Mitchell, Jodie Petty, Sophia Pickens, Amy Penird, LaPetra Robinson, Edwin Scheide, Tracy Starling, Joseph Trottier, Francis Ann Washington, Adam White, and Shawn White ("Plaintiffs"), on behalf of themselves and all others similarly situated ("Class Members"), bring this Class Action Complaint against TMX Finance Corporate Services, Inc., and TMX Finance LLC d/b/a "Title Max," "TitleBucks," and "InstaLoan" (collectively, "Defendants"[1] or "TMX"), Plaintiffs allege, based on their personal

[1] Plaintiffs anticipate that, through the process of discovery, they will discover additional individuals or entities who made decisions related to TMX's poor cybersecurity practices—such as the decision not to employ additional safeguards or logging, which could have prevented the data breach or discovered it before the hackers stole PII—and reserve the right to seek leave to amend to add them as defendants for their role in the data breach.

knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, the following:

NATURE OF THE CASE

1. Financial service providers that handle sensitive, personally identifying information ("PII") owe a duty to the individuals to whom that data relates. This duty arises based upon the parties' relationship and because it is foreseeable that exposure of PII to unauthorized persons—and especially to hackers with nefarious intentions—will result in harm to the affected individuals.

2. The exposure of sensitive PII to hackers, commonly referred to as a "data breach" causes material harm to its victims in several ways, often manifesting in identity theft and financial fraud, a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population (potentially for the rest of a victim's life), reputational harm, embarrassment, misuse of sensitive information, increased exposure to scams seeking to collect additional information, end even emotional distress. Mitigating the risk of even further harm, to the extent that it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit and financial accounts and take several additional prophylactic measures.[2]

3. Defendants are financial services providers that primarily provide short term, high-interest loans using vehicle titles as collateral. Defendant TMX Finance LLC is the parent company of TMX Finance Corporate Services, Inc. The TMX family of companies includes "TitleMax," "TitleBucks," and "InstaLoan" locations currently operating in 16 states. TMX

---

[2] *See* Federal Trade Commission, *What information was lost or exposed*, IdentityTheft.gov, https://www.identitytheft.gov/assets/pdf/Data_Breach.pdf (last accessed Nov. 28, 2023).

formerly operated in three additional states—California, Illinois, and Virginia—before closing all locations in those states between 2020 and 2023.

4. Plaintiffs bring this class action on behalf of themselves and approximately 4.8 million individuals whose personal information, including names, dates of birth, passport numbers, driver's license numbers, federal/state identification card numbers, tax identification numbers, Social Security numbers, financial account information, phone numbers, residential addresses, and email addresses (collectively, "Private Information" or "PII"), was accessed and stolen by unauthorized third parties during a data breach of TMX's network systems, which TMX states occurred between early December 2022 and February 14, 2023 (the "Data Breach").

5. In the ordinary course of business, Defendants stored and utilized Plaintiffs' and Class Members' Private Information. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. By voluntarily undertaking the collection of this sensitive Private Information, Defendants assumed a duty to use due care to protect that information.

6. Plaintiffs and Class Members had no choice in how Defendants stored their Private Information; often times, Plaintiffs and Class Members sought Defendants' services out of desperation. Unable to bargain the terms of their agreements, Plaintiffs and Class Members were given little choice but to have Defendants control how their data was used, stored, and disclosed—whether or not such usage, storage, and disclosure was contrary to Defendants' promises.

7. Despite their duty to protect Plaintiffs' and Class Members' Private Information, Defendants implemented inadequate data security procedures, safeguards, controls, and practices

with respect to collecting and storing Private Information on its computer systems. Foreseeably, cybercriminals exploited Defendants' data security vulnerabilities and exfiltrated Plaintiffs' and Class Members' Private Information from TMX's systems.

8. Hackers infiltrated TMX's computer systems on or around December 10, 2022, moved throughout the system, and ultimately exfiltrated Plaintiffs' and Class Members' PII between February 3 and February 14, 2023. Despite the fact that cybercriminals breached TMX's systems in early December 2022, TMX claims it only first detected suspicious activity on their systems on February 13, 2023—after the hackers had two months' of access to the systems and only after the hackers spent *ten days* stealing consumers' PII from TMX's computer systems.

9. TMX publicly confirmed that over 4.8 million consumers' PII, including Social Security numbers, was acquired by cybercriminals.

10. TMX waited a full 45 days after discovering the Data Breach to begin notifying those 4.8 million victims.

11. In late August 2023, TMX sent revised notices to Data Breach victims, informing them that the cybercriminals had actually stolen more information—including sensitive financial account information—from TMX's unsecured systems. This additional sensitive information included account numbers and credit/debit card numbers, including security codes, access codes, passwords, and PINs.

12. Cybercriminals possessed consumers' PII including Social Security numbers for ***nearly two months*** before Defendants notified victims of the Data Breach. Shockingly, cybercriminals possessed consumers' payment card information for ***over six months*** before

Defendants first notified victims that this sensitive information was also left unsecured and was stolen in the Data Breach.

13. As a direct and proximate result of TMX's implementation of inadequate data security safeguards and controls, its breach of duty to handle PII with reasonable care, and its failure to maintain the security of consumers' payment card information, Plaintiffs and nearly five million Class Members' PII is now in the hands of criminals.

14. As a result of TMX's conduct, Plaintiffs and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, the loss of value of their Private Information, and the substantial and imminent risk of identity theft. Given the theft of information that is immutable—such as Social Security numbers and dates of birth—this risk will remain with Plaintiffs and Class Members for the rest of their lives.

15. Upon information and belief, Plaintiffs' and Class Members' Private Information remains in TMX's possession. Plaintiffs and Class Members have a continuing interest in ensuring that information stored in TMX's systems is and remains safe from further exploitation.

16. Plaintiffs bring this class action lawsuit on behalf of themselves and all those similarly situated against TMX for its failure to adequately safeguard Plaintiffs' and Class Members' Private Information, which it collected, stored, and maintained on insufficiently-secured systems and databases, and for failing to provide adequate notice to Plaintiffs and Class Members that their information had been stolen by criminals.

17. To recover from TMX for these harms, Plaintiffs and the Class bring claims for negligence, negligence per se, breach of bailment, unjust enrichment, invasion of privacy, and

declaratory judgment, as well as numerous state statutory claims. Plaintiffs seek damages in an amount to be determined at trial and injunctive relief requiring TMX to, at minimum: 1) adopt and maintain reasonable data security measures to safeguard against future breaches of PII collected, stored, and maintained by TMX; and 2) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

18. Plaintiff **Sonya Albert** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Bartow County, Georgia.

19. Plaintiff **Makecia Berry** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Spalding County, Georgia.

20. Plaintiff **Ryan Carder** is a citizen of the State of Wisconsin, and at all times relevant to this action, resided and was domiciled in Fond du Lac County, Wisconsin.

21. Plaintiff **Sheneequa Carrington** is a citizen of the State of Virginia, and at all times relevant to this action, resided and was domiciled in Clarke County, Virginia.

22. Plaintiff **Lana Clark** is a citizen of the State of California, and at all times relevant to this action, resided and was domiciled in Los Angeles County, California.

23. Plaintiff **Victoria Coria** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Harris County, Texas.

24. Plaintiff **Antonio DeJesus** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Galveston County, Texas.

25. Plaintiff **Leon Diaz** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Harris County, Texas.

26. Plaintiff **Tommy Domino** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Harris County, Texas.

27. Plaintiff **Patsy Eslinger** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Floyd County, Georgia.

28. Plaintiff **Evelyn Francis** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Brooks County, Georgia.

29. Plaintiff **Jeremiah Gills** is a citizen of the State of Virginia, and at all times relevant to this action, resided and was domiciled in the City of Roanoke, Virginia.

30. Plaintiff **Dewayne Jackson** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Colquitt County, Georgia.

31. Plaintiff **Yolanda Jackson** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Dougherty County, Georgia.

32. Plaintiff **Adrian Johnson** is a citizen of the State of Alabama, and at all times relevant to this action, resided and was domiciled in Calhoun County, Alabama.

33. Plaintiff **Chaplin Johnson** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Lamar County, Texas.

34. Plaintiff **Von King** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Muscogee County, Georgia.

35. Plaintiff **Ebony Millner** is a citizen of the State of Virginia, and at all times relevant to this action, resided and was domiciled in the City of Martinsville, Virginia.

36. Plaintiff **Lakendra Mitchell** is a citizen of the State of Alabama, and at all times relevant to this action, resided and was domiciled in Bullock County, Alabama.

37. Plaintiff **Jodie Petty** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Atascosa County, Texas.

38. Plaintiff **Sophia Pickens** is a citizen of the State of Wisconsin, and at all times relevant to this action, resided and was domiciled in Milwaukee County, Wisconsin.

39. Plaintiff **Amy Penird** is a citizen of the State of Florida, and at all times relevant to this action, resided and was domiciled in Citrus County, Florida.

40. Plaintiff **LaPetra Robinson** is a citizen of the State of Missouri, and at all times relevant to this action, resided and was domiciled in Saint Louis County, Missouri.

41. Plaintiff **Edwin Scheide** is a citizen of the State of Illinois, and at all times relevant to this action, resided and was domiciled in Lake County, Illinois.

42. Plaintiff **Tracy Starling** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Cobb County, Georgia.

43. Plaintiff **Joseph Trottier** is a citizen of the State of Wisconsin, and at all times relevant to this action, resided and was domiciled in Kenosha County, Wisconsin.

44. Plaintiff **Francis Ann Washington** is a citizen of the State of Texas, and at all times relevant to this action, resided and was domiciled in Travis County, Texas.

45. Plaintiff **Adam White** is a citizen of the State of Tennessee, and at all times relevant to this action, resided and was domiciled in Scott County, Tennessee.

46. Plaintiff **Shawn White** is a citizen of the State of Georgia, and at all times relevant to this action, resided and was domiciled in Tift County, Georgia.

47. Defendant TMX Finance, LLC is a corporation organized under the laws of Delaware with its principal place of business at 15 Bull Street, Suite 200, Savannah, Georgia,

31401.[3] TMX Finance, LLC is a citizen of the States of Georgia and of Delaware. TMX Finance, LLC was founded in Savannah Georgia in June 2010 and was previously known as TMX Holdings, LLC.

48. TMX Finance, LLC's sole member is TMX Finance Holdings, Inc., a Delaware corporation with its principal place of business at 15 Bull Street, Suite 200, Savannah, Georgia 31401.[4] TMX Finance Holdings, Inc. is a citizen of the States of Georgia and of Delaware.

49. TMX Finance, LLC, is the parent company of Defendant TMX Finance Corporate Services, Inc. TMX Finance Corporate Services, Inc. is a corporation organized under the laws of Delaware with its headquarters and principal place of business at 15 Bull Street, Suite 200, Savannah, Georgia 31401.[5] Defendant TMX Finance Corporate Services, Inc. is a citizen of the States of Georgia and of Delaware.

50. TMX Finance Corporate Services, Inc., operates consumer credit and lending businesses, including TitleMax, which provides or provided personal loans as well as loans secured by auto and motorcycle titles to residents of Alabama, Arizona, California, Delaware, Georgia, Idaho, Illinois, Kansas, Mississippi, Missouri, Nevada, New Mexico, South Carolina, Tennessee, Texas, Utah, Virginia, and Wisconsin; InstaLoan, which offers loans secured by automobile titles, and short-term, high-interest personal loans to residents of Florida and New Mexico; and TitleBucks, which offers auto title loans to residents of Alabama, Arizona, Georgia, South Carolina, Tennessee, and Texas.

---

[3] May 14, 2013 Form 10Q, TMX Finance LLC, *available at* https://www.sec.gov/Archives/edgar/data/1511967/000110465913041451/a13-8662_110q.htm (last accessed Nov. 28, 2023).

[4] *Id.*

[5] *Id.*

JURISDICTION AND VENUE

51. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of Class Members exceeds 100, many of whom have different citizenship from Defendants, including several Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

52. This Court has personal jurisdiction over Defendant TMX Finance, LLC, and Defendant TMX Finance Corporate Services, Inc. because they operate and are headquartered in this District and conduct substantial business in this District. Defendant TMX Finance, LLC's sole member is also headquartered in this District and conducts substantial business in this District.

53. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendants are based in this District, maintain Plaintiffs' and Class Members' Private Information in this District, and have caused harm to Plaintiffs and Class Members in this District.

FACTUAL ALLEGATIONS

A. Defendants Know That Sharing Customer Information with Third Parties Can Cause or Is Likely to Cause Substantial Injury Due to Prior Bad Acts.

"The notion that [TitleMax's customers] [a]re reading [the contract] closely during a 15-minute transaction in a place with a neon sign" in the window is highly unlikely.
- John Campbell, Denver University Law Professor[6]

[6] Walker Moskop, *TitleMax is thriving in Missouri—and repossessing thousands of cars in the process*, St. Louis Post-Dispatch (Sept. 21, 2015), https://www.stltoday.com/news/local/metro/titlemax-is-thriving-in-missouri-and-repossessing-thousands-of-cars-in-the-process/article_d8ea72b3-f687-5be4-8172-9d537ac94123.html. Quotations below headings are not meant to prove the allegations in Plaintiffs' complaint, but

54. As acknowledged in court filings, despite the loans carrying harsh consequences (including, in at least Georgia, the inability to discharge the debts in bankruptcy[7]), the loan origination process for consumers "takes approximately thirty (30) to forty-five (45) minutes to complete."[8] Luring in customers with the promise of fast cash[9] if they own their own car, TMX does everything it can to avoid being transparent to its customers during the brief application process.[10]

55. Corporate training and sales techniques were created to confuse customers and trap them into an endless cycle of debt.[11] As part of its confusing sales practices, former store managers have also said that TMX's standard practice is to "simply show customers contracts on a digital screen, not in a physical copy."[12] At least one manager was reprimanded and told to stop printing sales contracts for his customers.[13]

---

demonstrate Defendants' ongoing culture of predatory practices, disregard for protecting sensitive information, and repeated violations of known duties.

7 Margaret Coker and Joel Jacobs, *TitleMax Demands High-Interest Payments from Borrowers in Bankruptcy*, ProPublica (July 13, 2023), https://www.propublica.org/article/why-title-lenders-excluded-chapter-13-bankruptcy-georgia.

8 Affidavit of John Robinson, President of the Debtors, in Support of First Day Motions and Applications, *In re TitleMax Holdings, LLC, et al.*, No. 09-40805-LWD, ECF No. 22 (S.D. Ga. Apr. 21, 2009), *available at* https://s3.documentcloud.org/documents/1227212/tmx-exec-delcaration-in-bk-case.pdf.

9 TitleMax TV Spot, "Car & Title," iSpot.tv, https://www.ispot.tv/ad/AEgc/titlemax-car-and-title (at 00:11-00:13, ". . .and you can get your cash in as little as thirty minutes!"; at 00:25, fine print stating that, "Most applications processed in about 30 minutes.").

10 Margaret Coker and Joel Jacobs, *How Title Lenders Trap Poor Americans in Debt with Triple-Digit Interest Rates*, ProPublica (Nov. 14, 2023), https://www.propublica.org/article/title-lenders-trap-georgia-residents-in-debt.

11 Margaret Coker, *Inside the Controversial Sales Practices of the Nation's Biggest Title Lender*, ProPublica (Jan. 19, 2023), https://www.propublica.org/article/inside-sales-practices-of-biggest-title-lender-in-us.

12 *Id.*

13 *Id.*

56. In 2016, the Consumer Financial Protection Bureau ordered TMX to pay a $9 million penalty because it "lured consumers into more expensive loans with information that hid the true costs of the deal."[14] As part of its findings, the CFPB also found that TMX had "exposed information about consumers' debts to co-workers, neighbors and family."[15] Specifically, the CFPB stated that:

> Some TMX Finance employees revealed information about consumers' past-due debt while visiting consumers' homes, references, or places of employment. TMX Finance also made in-person debt collection attempts despite knowing that visitors were not permitted at the consumer's workplace. Such visits can damage consumers' reputations, interfere with their ability to do their jobs, and trigger disciplinary action or firing.[16]

57. According to the CFPB's enforcement action, TMX's "employees disclosed the existence of consumers' past-due debts to third parties," and that TMX's "disclosure of the existence of consumers' debts to third parties caused or was likely to cause substantial injury to consumers that was not reasonably avoidable or outweighed by the countervailing benefit to consumers or to competition."[17]

58. TMX knew—since at least 2016—that the information it collected about consumers should not be shared with third parties. And, pursuant to the CFPB enforcement action, TMX also knew that disclosing its customers' Private Information—including that they owed money on a debt to TMX—was substantially likely to cause harm.

---

14 *CFPB Fines Titlemax Parent Company $9 Million for Luring Consumers Into More Costly Loans*, CFPB (Sept. 26, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-titlemax-parent-company-9-million-luring-consumers-more-costly-loans/.

15 *Id.*

16 *Id.*

17 *In the Matter of: TMX Finance LLC*, No. 2016-CFPB-0022 (C.F.P.B. Sept. 26, 2016), *available at* https://files.consumerfinance.gov/f/documents/092016_cfpb_TitleMaxConsentOrder.pdf.

59. As part of the CFPB consent decree with TMX, TMX was permanently restrained from:

a. "communicating with any person or entity in relation to the consumer's account, other than the consumer," save for limited circumstances; and

b. "disclosing the existence of the consumer's debt to any person other than the consumer," absent prior, express consent of the consumer.[18]

60. TMX's Board of Managers were charged with ensuring that TMX followed the provisions of the consent decree, including cessation of sharing information with third parties, the submission of compliance plans to the CFPB, and "corrective action to remedy any material non-compliance. . . ."[19]

61. TMX's cavalier attitude toward personal information did not stop in 2016. In February 2023, the CFPB found that TMX, in addition to violating the financial rights of military families and other consumers through predatory lending practices, also "alter[ed] the personal information of military borrowers to circumvent their protected status."[20]

62. As part of the CPFB's enforcement action, the CFPB specifically found that TMX "changed consumers' personally identifiable information" in order to evade service-member protections against predatory lending practices.[21] The CFPB found that TMX did not "conduct

---

18 *Id.* at 10-11.

19 *Id.* at 13.

20 *CFPB Orders TitleMax to Pay a $10 Million Penalty for Unlawful Title Loans and Overchargnig Military Families*, CFPB (Feb. 23, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-titlemax-to-pay-a-10-million-penalty-for-unlawful-title-loans-and-overcharging-military-families/.

21 *In the Matter of: TMX Finance LLC*, No. 2023-CFPB-0001 (C.F.P.B. Feb. 23, 2023), https://files.consumerfinance.gov/f/documents/cfpb_tmx-finance-llc_consent-order_2023-02.pdf.

any periodic monitoring or audits or its organization activity to ensure compliance" with certain lending laws, "allowing intentional misconduct and problematic practices to go unchecked."[22]

63. TMX has been warned—repeatedly—that its practices are unlawful, subject its customers to harm, and that its failure to ensure compliance with the law has led to repeated violations.

64. Despite these warnings, hackers accessed TMX's computer systems—unfettered and undetected by TMX—for *over two months*.

B. Defendants Knew the Risks of Collecting and Storing Valuable PII and the Foreseeable Harms of Exposing Private Information to Third Parties

"Our customers are decent, hardworking people. They aren't bums. But to TitleMax, they have just one purpose: Money."
- Cordelius Brown, former manager[23]

65. At all relevant times, TMX knew it was storing and permitting employees to use its computer systems to transmit valuable, sensitive PII and that, as a result, those systems would be attractive targets for cybercriminals.

66. The data that TMX stores is a treasure trove for cybercriminals and contains all of the necessary building blocks to commit financial fraud against an already-vulnerable population with few resources to detect or fight against fraud.

67. TMX required customers to entrust their sensitive PII to TMX as a condition of seeking and/or obtaining financial services. In the ordinary course of its business practices, TMX collected, stored, maintained, and used PII from each of its customers, including Plaintiffs and Class Members.

---

22 *Id.* at 14.

23 Margaret Coker, *Inside the Controversial Sales Practices of the Nation's Biggest Title Lender*, ProPublica (Jan. 19, 2023), https://www.propublica.org/article/inside-sales-practices-of-biggest-title-lender-in-us.

68. The PII that customers entrust with TMX includes Social Security numbers, government document numbers, dates of birth, phone numbers, physical and email addresses, and payment card information, all of which can be used to commit myriad financial and identity crimes.

69. The ramifications of TMX's failure to safeguard Plaintiffs' and the Class's PII are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

70. Additionally, the CFPB warned TMX about the dangers its customers face when sensitive information is shared with third parties.

71. The Federal Trade Commission defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[24] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[25]

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

73. PII is highly valued by criminals, as evidenced by the prices that such information commands on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, a single victim's personal information can be sold at a price ranging

---

24 17 C.F.R. § 248.201 (2013).

25 *Id.*

from $40 to $200, and bank details have a price range of $50 to $200.[26] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[27] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[28]

74. While credit and debit card numbers have significant value to cybercriminals, this value is limited because victims can cancel or close their credit and debit card accounts when they are notified of a breach. In contrast, victims whose immutable personal information is stolen—like Plaintiffs and Class Members victimized by the Data Breach—have no straightforward way of safeguarding themselves against ongoing fraud.

75. Accordingly, Personally Identifiable Information commands a much higher price on the black market than payment card data. As Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[29]

76. Moreover, there may be a time lag between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

---

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

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

[28] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

77. Data theft is not a hypothetical concern; in fact, the rate of cyberattacks has increased dramatically in recent years. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68 percent increase from 2020.[31]

78. Cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service issued a warning to potential targets to be aware of, and prepared for, a potential attack.[32]

79. Generally, "[c]ybercriminals choose their targets based on two conditions – maximum impact and maximum profit . . . [f]inancial institutions perfectly meet these conditions because they store highly valuable data, and their digital transformation efforts are creating greater opportunities for cyber attackers to access that data."[33]

80. 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 to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

81. The development of "Fullz" packages means stolen PII from a data breach can easily be used to link and identify it to victims' phone numbers, email addresses, and other

---

30 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf.

31 *See* 2021 Data Breach Annual Report at 6 (ITRC, Jan. 2022), *available at* https://notified.idtheftcenter.org/s.

32 *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974.

33 Edward Kost, *10 Biggest Data Breach in Finance [Updated August 2022]*, UpGuard, (Mar. 2, 2023), https://www.upguard.com/blog/biggest-data-breaches-financial-services.

unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package and sell it at a higher price, over and over.

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

83. According to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[35]

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

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

86. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use stolen PII. To protect themselves, data breach victims need to remain vigilant against unauthorized data use for years or even decades to come.

---

[34] Federal Bureau of Investigation, *2019 Internet Crime Report* at 3, https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf.

[35] *2019 Internet Crime Report Released*, Federal Bureau of Investigation (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

87. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take significant time, money, and patience to resolve the fallout.[36] The FTC treats 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(a) of the FTC Act.

88. Aside from the risks of identity theft and fraud, PII is also private property that has monetary value to data breach victims.

89. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[37]

90. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[38] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[39]

---

[36] *See* Taking Charge, What to Do If Your Identity is Stolen, Federal Trade Commission, at 3 (2012), https://www.govinfo.gov/content/pkg/GOVPUB-FT-PURL-gpo27431/pdf/GOVPUB-FT-PURL-gpo27431.pdf.

[37] Brad Brown, Kumar Kanagasabai, Prashant Pant & Gonçalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/capabilities/quantumblack/our-insights/capturing-value-from-your-customer-data.

[38] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[39] *Id.* at 25.

91. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [$2] for a date of birth, USD 8 for a Social Security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, Social Security number, credit record and military [record] is estimated to cost USD 55."[40]

92. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee-for-services-provided to monetizing their users' data—including user data that is not necessary for product or service, which she refers to as "behavioral surplus."[41]

93. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to users. Market exchanges have sprung up where individual users like Plaintiff can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.[42] Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[43]

94. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished when users discover how their data is being covertly intercepted, collected, used, and disclosed.

---

40 *Id.*

41 Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019).

42 Kevin Mercandante, *Ten Apps for Selling Your Data for Cash, Best Wallet Hacks* (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

43 Jacob Kastrenakes, *A new TikTok Clone hit the top of the App Store by paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival.

95. As Professors Acquisti, Taylor, and Wagman relayed in their 2016 article "The Economics of Privacy," published in the Journal of Economic Literature:

> Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, and consumption habits) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[44]

96. In other words, a successful cyberattack leaves criminals with a lucrative and readily monetized supply of PII—and deprives its victims of the exclusive use of their own information.

97. The documented increase in cyberattacks, combined with increasing monetary incentives that heighten the risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants, at the time of the Data Breach.

98. TMX recognizes this risk, as evidenced by the Privacy Policies it posts on its website, assuring customers that:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer and mobile application safeguards and secured files and buildings. We also maintain physical, electronic and procedural safeguards (i.e., computer virus protection software, firewalls, encryption). Only authorized employees have access. Customer access to electronically stored account documents and information is protected via customer-created or customer-specific usernames and passwords.[45]

---

[44] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Lit. 442, 444 (June 2016).

[45] *TitleMax Privacy Policy*, https://www.tmxdisclosures.com/titlemax/privacy-policy (last accessed Nov. 28, 2023); *TitleBucks Privacy Policy*, https://www.tmxdisclosures.com/titlebucks/privacy-policy (last accessed Nov. 28, 2023); *InstaLoan Privacy Policy*, https://www.tmxdisclosures.com/instaloan/privacy-policy (last accessed Nov. 28, 2023).

99. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the finance industry preceding the date of the Data Breach.

100. Plaintiffs and Class Members, as current and former customers of Defendants, relied on Defendants to keep their PII confidential and secure, to use their information for business purposes only, and to make only authorized disclosure of their information.

101. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting Plaintiffs' and Class Members' Private Information from foreseeable risks of disclosure to unauthorized parties. Defendants agreed to and undertook legal duties to securely store and maintain the Private Information of Plaintiffs and Class Members.

C. The Data Breach was Foreseeable

"You hate to see it happen. If you have a TitleMax title loan, you are screwed."
- Elaina Massey, attorney, on excluding TMX loans from bankruptcy repayment plans[46]

102. TMX were obligated to perform its business operations in accordance with industry standards with respect to Plaintiffs and the Class Members by implementing reasonable data security measures in order to not create a foreseeable risk of harm to Plaintiffs and the Class Members. Industry best practices places the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, TMX was the one responsible for adequately protecting the data that that it collected and stored.

---

[46] Margaret Coker, *TitleMax Demands High-Interest Payments from Borrowers in Bankruptcy*, ProPublica (July 13, 2023), https://www.propublica.org/article/why-title-lenders-excluded-chapter-13-bankruptcy-georgia.

103. TMX also had existing obligations to protect Plaintiffs' and Class Members' information from disclosure to third parties based upon a prior consent decree with the Consumer Financial Protection Bureau.

104. TMX understood its obligations and represented to the public that it was following the prior consent decree by stating that it "has complied with all prior direction from the Bureau."[47]

105. The injuries to Plaintiffs and the other Class Members were reasonably foreseeable to TMX because common law, statutes, a prior consent decree, and industry standards require TMX to safeguard and protect their computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the other Class Members' PII.

106. The injuries to Plaintiffs and the other Class Members also were reasonably foreseeable because TMX knew or should have known that their systems used for safeguarding PII were inadequately secured and that consumer PII could therefore be breached, accessed, and stolen by hackers and unauthorized third parties.

107. Additionally, it was foreseeable that the Data Breach would cause harm to Plaintiffs and the Class. Indeed, the Consumer Financial Protection Bureau informed TMX about the risk consumers faced when their PII was not protected or was shared with third parties.

108. Further, TMX was aware of the risk to consumers's PII because a separate Consumer Financial Protection Bureau consent decree informed TMX that it had inadequate monitoring to ensure compliance with certain lending laws.

---

47 *TitleMax Statement of CFPB Consent Order*, TMX Finance (Feb. 24, 2023), https://www.tmxfinancefamily.com/press-releases/titlemax-statement-on-cfpb-consent-order/.

109. As such, Defendants' own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class Members.

110. The injuries to Plaintiffs and the other Class Members also were reasonably foreseeable because TMX, all persons in data collecting industries, and a large portion of the general public are aware of the high and ever-increasing incidence of cyberattacks perpetrated against entities that collect PII and the substantial increased risk of harm arising out of the same.

111. As a result, Defendants left Plaintiffs' and Class Members' PII as an unguarded target for theft and misuse.

D. Defendants Choose to Do Business with Vulnerable Populations, Who Are Most at Risk in Data Breaches.

"I had a hardship. I was between a rock and a hard place."
- Gloria Whitaker, TMX customer[48]

112. Short-term, high-interest loans—like the ones TMX offers—are often the option of last resort for consumers—many of whom are facing emergencies and need to access money or credit quickly.[49] These consumers have few resources and little to no ability to negotiate the terms of their loans, what information is collected, how that information is used, or what kind of security measures are put into place to protect their information.

113. TMX knows that its average customers are individuals who are unable to obtain traditional bank loans—most title lenders argue that they provide a vital service to people denied

---

[48] Fred Sculte, *Lawmakers protect title loan firms while borrowers pay sky-high interest rates*, Center for Public Integrity (Dec. 9, 2015), https://publicintegrity.org/inequality-poverty-opportunity/lawmakers-protect-title-loan-firms-while-borrowers-pay-sky-high-interest-rates/.

[49] Federal Trade Commission, *What to Know About Payday and Car Title Loans*, https://consumer.ftc.gov/articles/what-know-about-payday-and-car-title-loans (last accessed Nov. 28, 2023).

credit by banks.[50]

114. The "vital service" TMX provides, however, ensures that customers can rarely, if ever, pay off their loans—not only are the interest rates staggeringly high (in the triple digits),[51] but TMX also convinces consumers to extend the term of their loans by paying a fixed monthly rate—which they do not mention only covers interest.[52] TMX traps customers into a debt cycle, while at the same time doing little to protect all of the sensitive information that it collects from its desperate customers.

115. The very same individuals that TMX targets in its unfair lending schemes are the those who face a greater risk of financial fraud and identity theft as a result of data breaches—like the one identified in this lawsuit.

116. Information gathered by hackers as part of a data breach is frequently used to commit further fraud, identity theft, and scams.

117. Financial insecurity is a major indicator as to whether an individual is more susceptible to fraud.

> Prior work by Anderson (2013) and AARP (2003) has indicated that individuals who are under financial strain might be more susceptible to scams, especially scams that promise financial rewards or an opportunity to get out of debt. In the present study, low household income ($50,000 and below) was significantly associated with engaging and losing money in a scam (p<.001).
>
> Victims were also significantly more likely to agree with the statement "I have too much debt right now" (meanvictim=3.6 meannon-victim=3.1 out of seven, p=.001). Levels of financial insecurity varied by scam type. For example, respondents who

---

50 Fred Sculte, *Giant title loan companies argue they are people too*, Center for Public Integrity (Feb. 22, 2016), https://publicintegrity.org/inequality-poverty-opportunity/giant-title-loan-companies-argue-they-are-people-too/.

51 Margaret Coker and Joel Jacobs, *How Title Lenders Trap Poor Americans in Debt With Triple-Digit Interest Rates*, ProPublica (Nov. 14, 2023), https://www.propublica.org/article/title-lenders-trap-georgia-residents-in-debt.

52 *Id.* For example, one customer signed a contract to receive a loan of $9,518 in exchange for a lien on his 2006 Honda Ridgeline truck, and after paying $25,000 over two years, was only paying interest. *Id.*

reported advance fee loan, investment, and sweepstakes/lottery/prizes scams were more likely than other reporters to show signs of financial insecurity.[53]

118. TMX's carelessness and failure to implement reasonable data security exposed an already-vulnerable population to even more harm.

E. Defendants Breached their Duty by Failing to Apply Reasonable Security Safeguards

"She didn't even have the screen towards me! She said, it's a whole lot of words, don't worry about it. I'll take care of it for you. I didn't see anything until she told me where to sign."
- Rodney Paylor, TitleMax customer, on not being able to see the agreement he signed[54]

119. Recognizing the risks and costs of cybercriminal activity, government agencies and industry groups have created reasonable data security protocols that organizations should use to safeguard sensitive information from exposure to cybercriminals.

120. Defendants breached their duty to Plaintiffs and Class Members by failing to implement these reasonable protocols.

121. The FBI recommends several measures for organizations like TMX to prevent and detect unauthorized cyberattacks, including that they:

- Implement an awareness and training program. Because end-users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

---

[53] *Exposed to Scams, What Separates Victims from Non-Victims?* at 7, FINRA Foundation, https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-what-separates-victims-from-non-victims_0_0.pdf.

[54] Max Diekneite, *TitleMax customer warns of deceptive car title loans*, WTO11 Savannah (May 4, 2023), https://www.wtoc.com/2023/05/04/titlemax-customer-warns-deceptive-car-title-loans/.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[55]

[55] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf.

122. The Microsoft Threat Protection Intelligence Team recommends several measures for organizations like TMX to prevent and detect unauthorized cyberattacks, including that they:

a. Secure internet-facing assets

   i. Apply latest security updates;

   ii. Use threat and vulnerability management;

   iii. Perform regular audit; remove privileged credentials.

b. Include IT Pros in security discussions

   i. Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.

c. Build credential hygiene

   i. Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.

d. Apply principle of least-privilege

   i. Monitor for adversarial activities;

   ii. Hunt for brute force attempts;

   iii. Monitor for cleanup of Event Logs;

   iv. Analyze logon events[56]

123. Additionally, the Federal Trade Commission ("FTC") has also promulgated numerous guides for businesses to highlight the importance of implementing reasonable data

[56] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

security practices. According to the FTC, the need for data security should be factored into all business decision making.

124. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information they collect and store; 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 any security problems.[57]

125. The FTC further recommends that companies not maintain PII 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.

126. 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

---

[57] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protetingpersonal-information.pdf.

127. As described above, experts studying cybersecurity routinely identify companies in the finance industry as being particularly vulnerable to cyberattacks because of the value of the PII they collect and maintain.

128. Several best practices have been identified that, at a minimum, should be implemented by service providers like TMX, including but not limited to: educating all employees; requiring strong passwords; implementing multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, *i.e.*, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

129. Based upon information and belief, and after a reasonable investigation based upon information publicly available, TMX failed to meet the minimum standards established by 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.

130. The foregoing frameworks provide existing and applicable industry standards in the finance industry, which applied at all relevant times. TMX failed to comply with these accepted standards, thereby opening the door to the foreseeable risk of a Data Breach.

131. BecauseTMX was storing the PII of Plaintiffs and Class Members, TMX could and should have implemented the reasonable measures outlined above to prevent and detect cyberattacks. Instead, TMX implemented inadequate and less than basic security measures.

132. TMX's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

133. TMX was always fully aware of its obligations to protect the PII of their customers, including Plaintiffs' and Class Members. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. Defendants' Breach of Duty Was the Proximate Cause of the Data Breach

"The fact is, TitleMax misled plenty of employees in order to mislead the community."
- Cordelius Brown, former manager[58]

134. In or around early December 2022, an intruder gained unauthorized access to TMX's computer network.[59] TMX failed to detect the unauthorized access for more than two months.

135. Between February 3 and February 14, 2023, the intruder accessed and exfiltrated the PII of over 4.8 million customers.[60]

136. Despite learning on or before March 1, 2023 that Plaintiffs' and Class Members' PII had been stolen, Defendants did not notify Plaintiffs, Class Members, government officials, or the public of the Data Breach until March 30, 2023.

---

[58] Max Diekneite, *'At the end of the day, it's about the money:' Former TitleMax employee discusses sales practices*, WTOC11 Savannah (Aug. 25, 2023), https://www.wtoc.com/2023/08/25/end-day-its-about-money-former-titlemax-employee-discusses-sales-practices/.

[59] *TMX Finance Notice of Data Breach* (Mar. 30, 2023), https://s3.documentcloud.org/documents/23735720/tmx-finance-sample-copy-of-individual-notice-l01.pdf.

[60] *See id.*

137. On or around March 30, 2023, Defendants dispatched Data Breach Notice Letters ("March Notice") to Plaintiffs and Class Members, informing them that unauthorized actors were able to access and acquire sensitive personal information from Defendants' systems.[61]

138. The March Notice that Defendants sent to Plaintiffs and Class Members reads, in relevant part:

> **What Happened?** On February 13, 2023, we detected suspicious activity on our systems and promptly took steps to investigate the incident. As part of that investigation, global forensic cybersecurity experts were retained. Based on the investigation to date, the earliest known breach of TMX's systems started in early December 2022. On March 1, 2023, the investigation confirmed that information may have been acquired between February 3, 2023 – February 14, 2023. We promptly began a review of potentially affected files to determine what information may have been involved in this incident. We notified the FBI but have not delayed this notification for any law enforcement investigation.
>
> **What Information Was Involved?** The personal information involved may have included your name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, social security number and/or financial account information, and other information such as phone number, address, and email address.[62]

139. On or around August 23, 2023, Defendants dispatched an updated Data Breach Notice Letters ("August Notice") to Plaintiffs and Class Members, informing them that in addition to the PII referenced in the March Notice, cybercriminals had also stolen financial and payment card information—including account numbers, access codes, credit and debit card numbers, passwords, and PINs—from Defendants' unsecured systems.

---

61 *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/list.shtml (search for "TMX" and select entry dated "2023-03-30").

62 *TMX Finance Notice of Data Breach*, https://s3.documentcloud.org/documents/23735720/tmx-finance-sample-copy-of-individual-notice-l01.pdf (last accessed Nov. 28, 2023)

140. The August Notice[63] did not explain to Plaintiffs and Class Members the reason for the delay in notifying them of the theft of their payment card information. Either Defendants' February investigation of the Data Breach, which Defendants claim was conducted by global forensic cybersecurity experts, failed to discover that cybercriminals had stolen payment card information from Defendants' systems; or Defendants actually discovered the theft of payment card information in March 2023 and failed to notify Plaintiffs, Class Members, government agencies and the public until August 2023.

141. As a result of Defendants' failure to either discover or notify Plaintiffs and Class Members about the scope of the Data Breach, cybercriminals had unfettered access to Plaintiffs' and Class Members' payment card information for at least six months before Plaintiffs and Class Members even knew that this sensitive information had been stolen from Defendants' network.

142. Because TMX failed to properly protect and safeguard Plaintiffs' and Class Members' Private Information, unauthorized third parties were able to access Defendants' computer systems and exfiltrate Plaintiffs' and Class Members' Private Information stored therein.

143. TMX could have prevented the Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members.

144. Alternatively, TMX could have destroyed the data, especially for individuals who had fulfilled their contractual obligations with Defendants and no longer had a business relationship with TMX.

---

63 *Available at* https://apps.web.maine.gov/online/aeviewer/ME/40/c5a6aaa4-3626-4fe0-9dda-5a32a18fe814/40327988-f6c2-4a50-b55a-3e35a8d389b8/document.html.

145. TMX could have prevented or mitigated the harm of the Data Breach by monitoring event logs and discovering suspicious activity when it first occurred in December 2022, two months before Plaintiffs' and Class Members' PII was exfiltrated in February 2023.

146. TMX could have mitigated the harm of the Data Breach by timely discovering and reporting the theft of payment card information, instead of waiting to notify Plaintiffs and Class Members until August 2023—*six months* after the theft had occurred.

147. TMX's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like TMX to protect and secure sensitive data they possess. Despite the prevalence of public announcements regarding data breach and data security threats, TMX implemented inadequate measures and controls to protect the PII of Plaintiffs and Class Members from compromise.

G. Plaintiffs and Class Members Suffered Injury

"We are deeply concerned that TMX Finance's predatory behavior concerning title loans continued while under an active consent decree and seek further information on whether this new order will prevent similar predatory behavior going forward."
- *Senators Ben Ray Lujan, Elizabeth Warren, Robert P. Casey, Alex Padilla, and Bernard Sanders*[64]

148. As a direct and proximate result of TMX's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft, as well as other, acknowledged harms that occur as a result of sharing sensitive information with third parties.

149. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

---

[64] Letter to Director Rohit Chopra, Consumer Financial Protection Bureau (Mar. 14, 2023), https://www.lujan.senate.gov/wp-content/uploads/2023/03/CFPB-TitleMax-Letter.pdf.

150. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information. Potential fraudsters can use the Private Information compromised in the Data Breach to more effectively target such schemes to Plaintiffs and Class Members.

151. Additionally, Plaintiffs and Class Members face embarrassment and humiliation resulting from information related to high-interest and high-pressure loans being shared with third parties. Unfortunately, in order to protect their rights and the rights of absent Class Members, Plaintiffs must subject themselves to embarrassment yet again by filing this lawsuit disclosing that they used TMX's services.

152. Plaintiffs and Class Members now face years of constantly monitoring their financial and personal records to protect themselves from fraud and identity theft. Indeed, even Defendants recommend that Plaintiffs and Class Members "stay vigilant" and continue to monitor their financial information.[65] The Class is incurring and will continue to incur such damages in addition to any economic losses resulting from fraudulent use of their PII.

153. Defendants' delay in notifying affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

154. Plaintiffs and Class Members have suffered and will suffer actual injury and damages as a direct result of the Data Breach. Many victims, including Plaintiffs and Class

---

[65] *See* March Breach Notification Letter, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/179ab0ce-2c43-4119-ae5a-db766d4be3e0/10c498f9-1367-4030-bacc-e5698f177f13/document.html ("We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid."); and August Breach Notification Letter, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/c5a6aaa4-3626-4fe0-9dda-5a32a18fe814/40327988-f6c2-4a50-b55a-3e35a8d389b8/document.html (same)

Members, suffered ascertainable losses in the form of out-of-pocket expenses and the value of lost time reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security number, bank accounts, and credit reports for unauthorized activity for years to come.

155. TMX specifically recommended that Plaintiffs and Class Members take these actions to protect themselves.

156. Moreover, Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, ensuring the storage of data or documents containing Private Information is not accessible online and that access to such data is encrypted and password protected.

157. Upon information and belief, TMX's computer systems are still at risk of hacking by unauthorized individuals who may easily access the Private Information of Plaintiffs and Class Members.

158. To date, Defendants have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

159. Defendants acknowledge the harm caused to Plaintiffs and Class Members because they offer a complimentary 12-month credit monitoring program via Experian IdentityWorks. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate, as it fails to account for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

160. TMX places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, instead of automatically enrolling all victims of the Data Breach.

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

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

b. The loss 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 of 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 Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in their possession.

162. In addition, the stolen PII may fall into the hands of companies who will use the information for targeted marketing, without obtaining consent from, or providing compensation to, Plaintiffs and Class Members.

H. Plaintiffs' Experiences

". . . .TitleMax actively works to make its contracts as confusing as possible and punishes employees who dare to actually explain to customers what they're getting themselves into. Which seems pretty evil."[66]

Plaintiff Sonya Albert

163. Plaintiff Sonya Albert is an adult individual and a natural person of Georgia, residing in Bartow County, where she intends to stay. Plaintiff Sonya Albert received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff Albert that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

---

66 Collin Woodward, *How TitleMax Makes Sure Customers Can Never Pay Off Their Car Loans*, Jalopnik (Jan. 19, 2023), *available at* https://jalopnik.com/how-titlemax-makes-sure-customers-can-never-pay-off-the-1850006898.

164. Plaintiff Albert only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

165. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Albert suffered injury from a loss of privacy.

166. Plaintiff Albert has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

167. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals, as a direct and proximate result of Defendants' misconduct.

168. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Albert, the Data Breach has forced her to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

169. Defendants acknowledged the risk posed to Plaintiff Albert and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy

and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

170. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Albert to suffer stress, fear, and anxiety.

171. Plaintiff Albert has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Makecia Berry

172. Plaintiff Makecia Berry is an adult individual and a natural person of Georgia, residing in Spalding County, where she intends to stay. Plaintiff Berry received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff Berry that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

173. Plaintiff Berry only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

174. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

175. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

176. Plaintiff Berry has experienced an increase in spam calls and emails since the Data Breach.

177. The Data Breach has also caused Plaintiff Berry to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

178. Defendants acknowledged the risk posed to Plaintiff and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

179. Plaintiff Berry has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Ryan Carder

180. Plaintiff Ryan Carder is an adult individual and a natural person of Georgia, residing in Fond du Lac County, where he intends to stay. Plaintiff Carder received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff Carder that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social

Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

181. Plaintiff Carder only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

182. Defendants sent Plaintiff Carder a Data Breach Notice Letter. After receiving the letter, Plaintiff Carder called Defendants to request any records in their possession, but he was told that Defendants could not find his accounts, causing him added anxiety and stress.

183. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Carder suffered injury from a loss of privacy.

184. Plaintiff Carder has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

185. Upon information and belief, Plaintiff Carder's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Carder's life.

186. Furthermore, Plaintiff has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach.

187. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and

misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

188. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Carder has taken steps to replace his debit card, close multiple bank accounts, and reset automatic billing instructions on various of his accounts because of the Data Breach.

189. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Carder, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

190. Defendants acknowledged the risk posed to Plaintiff Carder and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

191. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety related to his online security.

192. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Sheneequa Carrington

193. Plaintiff Sheneequa Carrington is an adult individual and a natural person of Virginia, residing in Clarke County, Virginia, where she intends to stay. Plaintiff Carrington received a notice letter from Defendants, informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

194. Plaintiff Carrington has experienced a drastic increase in spam emails, texts, and telephone calls as a result of the Data Breach.

195. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

196. Plaintiff Carrington only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

197. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

198. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This

information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

199. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Carrington, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

200. Defendants acknowledged the risk posed to Plaintiff Carrington and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

201. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

202. Plaintiff Carrington has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Lana Clark

203. Plaintiff Lana Clark is an adult individual and a natural person of California, residing in Los Angeles County, where she intends to stay. Plaintiff Clark received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security

number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

204. Plaintiff Clark only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

205. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

206. Plaintiff Clark has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

207. Upon information and belief, Plaintiff Clark's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft. Plaintiff Clark has also experienced credit issues.

208. Plaintiff Clark also experienced a drastic increase in spam emails and telephone calls as a result of the Data Breach.

209. The Data Breach caused Plaintiff Clark to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

210. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Clark, the Data Breach has forced Plaintiff Clark to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

211. Defendants acknowledged the risk posed to Plaintiff Clark and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

212. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Clark to suffer stress, fear, anxiety, and emotional distress.

213. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Victoria Coria

214. Plaintiff Victoria Coria is an adult individual and a natural person of Texas, residing in Harris County, where she intends to stay. Plaintiff Coria received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

215. Plaintiff Coria only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

216. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

217. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

218. The Data Breach has caused Plaintiff Coria to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

219. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Coria, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

220. Defendants acknowledged the risk posed to Plaintiff Coria and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy

and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

221. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

222. Plaintiff Coria has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Antonio DeJesus

223. Plaintiff Antonio DeJesus is an adult individual and a natural person of Texas, residing in Galveston County, where he intends to stay. Plaintiff DeJesus received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff DeJesus that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

224. Plaintiff DeJesus only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

225. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

226. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

227. Upon information and belief, Plaintiff DeJesus's Private Information has already been stolen and misused as a result of the Data Breach, as he has already experienced incidents of fraud and identity theft. The foregoing has detrimentally impacted Plaintiff DeJesus's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

228. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

229. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff DeJesus, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

230. Defendants acknowledged the risk posed to Plaintiff DeJesus and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

231. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety requiring medical attention.

232. Plaintiff DeJesus has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Leon Diaz

233. Plaintiff Leon Diaz is an adult individual and a natural person of Texas, residing in Harris County, where he intends to stay. Plaintiff Diaz received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

234. Plaintiff Diaz only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

235. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

236. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This

information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

237. Upon information and belief, Plaintiff Diaz's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced incidents of fraud and identity theft. The foregoing has detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

238. The Data Breach has also caused Plaintiff Diaz to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

239. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Diaz, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

240. Defendants acknowledged the risk posed to Plaintiff Diaz and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

241. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Diaz to suffer stress, fear, and anxiety. Plaintiff Diaz has experienced worsening depression and

PTSD following the Data Breach, requiring regular medical attention and prescription medication.

242. Plaintiff Diaz has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Tommy Domino

243. Plaintiff Tommy Domino is an adult individual and a natural person of Texas, residing in Harris County, where he intends to stay. Plaintiff Domino received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

244. Plaintiff Domino only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

245. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

246. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This

information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

247. Upon information and belief, Plaintiff Domino's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced incidents of fraud and identity theft, and has also experienced increased phishing and spam activity, including hourly spam emails and telephone calls.

248. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

249. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Domino, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

250. Defendants acknowledged the risk posed to Plaintiff Domino and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

251. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer an extreme increase in stress and anxiety.

252. Plaintiff Domino has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Patsy Eslinger

253. Plaintiff Patsy Eslinger is an adult individual and a natural person of Georgia, residing in Floyd County, where she intends to stay. Plaintiff Eslinger received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

254. Plaintiff Eslinger only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

255. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Eslinger suffered injury from a loss of privacy.

256. Plaintiff Eslinger has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

257. Upon information and belief, Plaintiff Eslinger's Private Information has already been stolen and misused as a result of the Data breach, as she has increased spam and phishing attempts.

258. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

259. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Eslinger, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

260. Defendants acknowledged the risk posed to Plaintiff Eslinger and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

261. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Eslinger to suffer stress, fear, and anxiety. Plaintiff has experienced worsening depression, requiring regular medical attention and prescription medication, following the Data Breach.

262. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Evelyn Francis

263. Plaintiff Evelyn Francis is an adult individual and a natural person of Georgia, residing in Brooks County, where she intends to stay. Plaintiff Francis received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

264. Plaintiff Francis only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

265. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

266. Plaintiff Francis has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

267. Upon information and belief, Plaintiff Francis's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft. These actions by unauthorized criminal third parties have detrimentally

impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

268. Furthermore, Plaintiff Francis has experienced a drastic increase in spam emails and telephone calls as a result of the Data Breach.

269. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

270. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Francis, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

271. Defendants acknowledged the risk posed to Plaintiff Francis and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

272. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

273. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Jeremiah Gills

274. Plaintiff Jeremiah Gills is an adult individual and a natural person of Virginia, residing in the City of Roanoke, where he intends to stay. Plaintiff Gills received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

275. Plaintiff Gills only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

276. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

277. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

278. Plaintiff has experienced fraudulent debit card charges and an increase in spam emails and phishing attempts as a result of the Data Breach.

279. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and

misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

280. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Gills, the Data Breach has forced him to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

281. Defendants acknowledged the risk posed to Plaintiff Gills and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

282. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

283. Plaintiff Gills has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Melvin Nicholas

284. Plaintiff Melvin Nicholas is an adult individual and a natural person of Nevada, residing in Clark County, where he intends to stay. Plaintiff Nicholas received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff Nicholas that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number,

Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

285. Plaintiff Nicholas only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

286. In the instant that his Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Nicholas suffered injury from a loss of privacy.

287. Plaintiff Nicholas has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

288. Upon information and belief, Plaintiff Nicholas's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced incidents of fraud and identity theft.

289. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals, as a direct and proximate result of Defendants' misconduct.

290. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Nicholas, the Data Breach has forced him to spend significant time and

energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

291. Defendants acknowledged the risk posed to Plaintiff Nicholas and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

292. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Nicholas to suffer stress, fear, and anxiety.

293. Plaintiff Nicholas has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff DeWayne Jackson

294. Plaintiff DeWayne Jackson is an adult individual and a natural person of Georgia, residing in Colquitt County, where he intends to stay. Plaintiff Jackson received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

295. Plaintiff Jackson only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his

Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

296. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Jackson suffered injury from a loss of privacy.

297. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

298. Upon information and belief, Plaintiff Jackson's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced fraudulent transactions.

299. Plaintiff Jackson also experienced a drastic increase in spam activity, including spam emails, telephone calls and text messages, requiring him to create a new email account due to the volume of spam emails.

300. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

301. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Jackson, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the

legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

302. Defendants acknowledged the risk posed to Plaintiff and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

303. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

304. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Yolanda Jackson

305. Plaintiff Yolanda Jackson is an adult individual and a natural person of Georgia, residing in Dougherty County, where she intends to stay. Plaintiff Jackson received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff Jackson that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

306. Plaintiff Jackson only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access

databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

307. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

308. Plaintiff Jackson has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

309. Upon information and belief, Plaintiff Jackson's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft. The foregoing has detrimentally impacted Plaintiff Jackson's life as a whole, and specifically caused financial strain on her.

310. Furthermore, Plaintiff has experienced a drastic increase in spam emails, telephone calls, and phishing attempts as a result of the Data Breach.

311. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

312. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Jackson, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports

to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

313. Defendants acknowledged the risk posed to Plaintiff and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

314. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

315. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Adrian Johnson

316. Plaintiff Adrian Johnson is an adult individual and a natural person of Alabama, residing in Calhoun County, where he intends to stay. Plaintiff Johnson received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

317. Plaintiff Johnson only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access

databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

318. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

319. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

320. Upon information and belief, Plaintiff Johnson's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced fraudulent transactions.

321. Additionally, Plaintiff has experienced a drastic increase in spam telephone calls as a result of the Data Breach.

322. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

323. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Johnson, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

324. Defendants acknowledged the risk posed to Plaintiff Johnson and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

325. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

326. Plaintiff Johnson has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Chaplin Johnson

327. Plaintiff Chaplin Johnson is an adult individual and a natural person of Texas, residing in Lamar County, where he intends to stay. Plaintiff Johnson received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

328. Plaintiff Johnson only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

329. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Johnson suffered injury from a loss of privacy.

330. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

331. Upon information and belief, Plaintiff Johnson's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced incidents of fraud and identity theft.

332. Furthermore, Plaintiff has experienced an increase in spam telephone calls and spam emails as a result of the Data Breach.

333. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

334. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Johnson, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

335. Defendants acknowledged the risk posed to Plaintiff Johnson and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

336. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

337. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Von King

338. Plaintiff Von King is an adult individual and a natural person of Georgia, residing in Muscogee County, where he intends to stay. Plaintiff King received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

339. Plaintiff King only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

340. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

341. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

342. Upon information and belief, Plaintiff King's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced incidents of fraud and identity theft .

343. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

344. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff King, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

345. Defendants acknowledged the risk posed to Plaintiff and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

346. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

347. Plaintiff King has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Ebony Millner

348. Plaintiff Ebony Millner is an adult individual and a natural person of Virginia, residing in the City of Martinsville, where she intends to stay. Plaintiff Millner received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach..

349. Plaintiff Millner only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

350. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

351. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This

information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

352. Upon information and belief, Plaintiff Millner's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft. The foregoing has detrimentally impacted Plaintiff Millner's life as a whole, and specifically caused financial strain on her.

353. Furthermore, Plaintiff has experienced a drastic increase in spam telephone calls and text messages as a result of the Data Breach.

354. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

355. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Millner, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

356. Defendants acknowledged the risk posed to Plaintiff Millner and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

357. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Millner to suffer stress, fear, and anxiety, requiring her to seek medical attention and prescription medication to treat depression, anxiety and panic attacks, as a result of the Data Breach.

358. Plaintiff Millner has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Lakendra Mitchell

359. Plaintiff Lakendra Mitchell is an adult individual and a natural person of Alabama, residing in Bullock County, where she intends to stay. Plaintiff Mitchell received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

360. Plaintiff Mitchell only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

361. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

362. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This

information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

363. Plaintiff has experienced an increase in spam activityas a result of the Data Breach.

364. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

365. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Mitchell, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, freezing her credit, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

366. Defendants acknowledged the risk posed to Plaintiff Mitchell and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

367. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

368. Plaintiff Mitchell has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Jodie Petty

369. Plaintiff Jodie Petty is an adult individual and a natural person of Texas, residing in Atascosa County, where she intends to stay. Plaintiff Petty received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

370. Plaintiff Petty only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

371. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

372. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

373. Since the Data Breach, Plaintiff Petty has experienced a drastic increase in spam activity and phishing emails, and a reduction in her credit score.

374. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and

misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

375. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Petty, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, freezing her credit, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

376. Defendants acknowledged the risk posed to Plaintiff Petty and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

377. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

378. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Sophia Pickens

379. Plaintiff Sophia Pickens is an adult individual and a natural person of Wisconsin, residing in Milwaukee County, where she intends to stay. Plaintiff Pickens received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number,

Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

380. Plaintiff Pickens only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

381. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

382. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

383. Upon information and belief, Plaintiff Pickens's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft . The foregoing has detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her.

384. Furthermore, Plaintiff Pickens experienced a drastic increase in spam telephone calls, spam emails and suspicious letters in the mail following the Data Breach.

385. The Data Breach has also caused Plaintiff Pickens to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

386. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Pickens, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, disputing charges, and self-monitoring her accounts and credit reports. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

387. Defendants acknowledged the risk posed to Plaintiff Pickens and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

388. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Pickens to suffer stress, fear, anxiety, and depression as a result of the Data Breach.

389. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Amy Penird

390. Plaintiff Amy Penird is an adult individual and a natural person of Florida, residing in Citrus County, where she intends to stay. Plaintiff Penird received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

391. Plaintiff Penird only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

392. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

393. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

394. Plaintiff Penird has experienced a drastic increase in spam activity, including thousands of spam emails and telephone calls since the Data Breach.

395. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

396. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Penird, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

397. Defendants acknowledged the risk posed to Plaintiff Penird and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

398. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

399. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff LaPetra Robinson

400. Plaintiff LaPetra Robinson is an adult individual and a natural person of Missouri, residing in St. Louis County, where she intends to stay. Plaintiff Robinson received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

401. Plaintiff Robinson only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

402. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

403. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

404. Upon information and belief, Plaintiff Robinson's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft. The foregoing has detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her.

405. Furthermore, Plaintiff Robinson has experienced a drastic increase in spam emails, spam telephone calls, and phishing attempts since the Data Breach.

406. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

407. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Robinson, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

408. Defendants acknowledged the risk posed to Plaintiff and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

409. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

410. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Edwin Scheide

411. Plaintiff Edwin Scheide is an adult individual and a natural person of Illinois, residing in Lake County, where he intends to stay. Plaintiff Scheide received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

412. Plaintiff Scheide only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

413. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

414. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

415. Upon information and belief, Plaintiff Scheide's Private Information has already been stolen and misused as a result of the Data Breach, as he has experienced incidents of fraud and identity theft.

416. Furthermore, Plaintiff has experienced increased spam activity and phishing attempts since the Data Breach.

417. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

418. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Scheide, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

419. Defendants acknowledged the risk posed to Plaintiff Scheide and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy

and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

420. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

421. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Tracy Starling

422. Plaintiff Tracy Starling is an adult individual and a natural person of Georgia, residing in Cobb County, where she intends to stay. Plaintiff Starling received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

423. Plaintiff Starling only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

424. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

425. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

426. Upon information and belief, Plaintiff Starling's Private Information has already been stolen and misused as a result of the Data Breach, as she has experienced incidents of fraud and identity theft. The foregoing has detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her.

427. Furthermore, Plaintiff has experienced a drastic increase in spam emails and telephone calls since the Data Breach.

428. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

429. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Starling, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

430. Defendants acknowledged the risk posed to Plaintiff Starling and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy

and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

431. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

432. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Joseph Trottier

433. Plaintiff Joseph Trottier is an adult individual and a natural person of Wisconsin, residing in Kenosha County, where he intends to stay. Plaintiff Trottier received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

434. Plaintiff Trottier only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

435. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

436. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

437. Plaintiff Trottier has experienced a drastic increase in spam activity and phishing attempts, including approximately 10-15 spam telephone calls a day, following the Data Breach.

438. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

439. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Trottier, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

440. Defendants acknowledged the risk posed to Plaintiff Trottier and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

441. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

442. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Francis Ann Washington

443. Plaintiff Francis Ann Washington is an adult individual and a natural person of Texas, residing in Travis County, where she intends to stay. Plaintiff Washington received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

444. Plaintiff Washington only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

445. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

446. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

447. Plaintiff Washington has experienced a drastic increase in spam activity and phishing attempts following the Data Breach.

448. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

449. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff Washington, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

450. Defendants acknowledged the risk posed to Plaintiff Washington and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

451. The substantial risk of imminent harm and loss of privacy have caused Plaintiff Washington to suffer stress, fear, and anxiety.

452. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Adam White

453. Plaintiff Adam White is an adult individual and a natural person of Tennessee, residing in Scott County, where he intends to stay. Plaintiff White received a notice letter from Defendants informing him of the Data Breach and the exposure of his Private Information. The notice letter informed Plaintiff that his name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

454. Plaintiff White only allowed Defendants to maintain, store, and use his Private Information because he believed Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

455. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

456. Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was made accessible to and exfiltrated by cybercriminals.

457. Upon information and belief, Plaintiff White's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft.

458. Plaintiff White has also experienced a drastic increase in spam activity and phishing attempts inquiring about loan information following the Data Breach.

459. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of his Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

460. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff White, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

461. Defendants acknowledged the risk posed to Plaintiff and his Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

462. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

463. Plaintiff White has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Shawn White

464. Plaintiff Shawn White is an adult individual and a natural person of Georgia, residing in Tift County, where she intends to stay. Plaintiff White received a notice letter from Defendants informing her of the Data Breach and the exposure of her Private Information. The

notice letter informed Plaintiff that her name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, phone number, address, and email address were potentially compromised in the Data Breach.

465. Plaintiff White only allowed Defendants to maintain, store, and use her Private Information because she believed Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

466. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

467. Plaintiff has been further injured by the damages to and loss in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was made accessible to and exfiltrated by cybercriminals.

468. Plaintiff White has experienced a drastic increase in spam telephone calls and phishing attempts following the Data Breach.

469. The Data Breach has also caused Plaintiff White to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse of her Private Information, which is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

470. In addition to the actual harm and substantially increased risk of future harm suffered by Plaintiff White, the Data Breach has forced Plaintiff to spend significant time and

energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

471. Defendants acknowledged the risk posed to Plaintiff White and her Private Information as a result of the Data Breach, both by explicitly stating that "TMX takes the privacy and security of your personal information very seriously" and by offering a 12-month identity theft protection service.

472. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

473. Plaintiff White has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected, and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

474. Plaintiffs bring this case as a class action on behalf of themselves and on behalf of a Nationwide Class ("the Class"), and on behalf of certain State Subclasses, specifically, a California Subclass, a Wisconsin Subclass, a Georgia Subclass, a Texas Subclass, an Alabama Subclass, an Illinois Subclass, a Virginia Subclass, a Florida Subclass, a Missouri Subclass, a Tennessee Subclass, and a Nevada Subclass pursuant to Rule 23(b)(2) and/or 23(b)(3) of the Federal Rules of Civil Procedure:

475. **Nationwide Class:** All individuals in the United States whose Private Information was actually or potentially accessed or acquired during the TMX Data Breach and for which Defendants provided notice to Plaintiffs and other Class Members beginning on or around March

30, 2023 (the "Nationwide Class" or "Class") as identified by Defendants' records relating to the Data Breach .

476. **State Subclasses**. All residents of a particular state[67] whose Private Information was actually or potentially accessed or acquired during the TMX Data Breach and for which Defendants provided notice to Plaintiffs and other Subclass Members beginning on or around March 30, 2023.

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

478. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

479. The Class and Subclasses each satisfy the prerequisites for class certification under Fed. R. Civ. P. 23(a).

480. **Numerosity**: Class Members are so numerous that joinder of all members is impracticable. Defendants have asserted that there are over 4.8 million individuals whose Private Information was improperly accessed in the Data Breach. Upon information and belief, each Subclass includes at least several thousand individuals. The exact size of the Class and the identities and state citizenship of each Class Member is ascertainable from Defendants' records.

---

[67] As described herein, California, Wisconsin, Georgia, Texas, Alabama, Illinois, Virginia, Florida, Missouri, Tennessee, and Nevada each have a state Subclass.

481. **Commonality**: This action involves questions of law and fact common to the Class and State Subclasses. Such common questions include, but are not limited to:

a. Whether Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants breached its duty to safeguard the Private Information of Plaintiffs and Class Members;

d. Whether and when Defendants actually learned of the Data Breach;

e. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

f. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

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

h. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

i. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

j. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

482. **Typicality**: Plaintiffs' claims are typical of those of the Class Members and of the Subclass Members from the State they represent. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiffs and Class Members were all customers of Defendants, each having their PII compromised due to Defendant's conduct.

483. **Adequacy of Representation**: Plaintiffs are adequate representatives of the Class and Subclasses because their interests do not conflict with the interests of other Class Members; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Class Members' interests will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

484. The Class and Subclasses each satisfy the criteria for class certification under Fed. R. Civ. P. 23(b)(3).

485. **Predominance**: Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. TMX has engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by TMX's actions and failure to act with respect to its collecting and storing the Private Information and its implementation of security procedures, safeguards, controls, and practices to protect such information, as well as TMX's failure to timely alert affected patients to the Data Breach. These

common issues predominate over any individual questions and are apt to drive the resolution of this litigation.

486. **Superiority**: Class litigation is the superior method for fair and efficient adjudication of the claims involved. Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making class action superior to individual action.

487. **Manageability**: Defendants assert that there are more than 4.8 million individuals whose PII was compromised in the Data Breach. The claims of Plaintiffs and Class Members are substantially identical as explained above. Thus, even if Class Members had the resources to pursue individual lawsuits, the judicial system does not have the resources to hear them. Certifying the case as a class action will centralize millions of substantially identical claims in a single proceeding, making a class action the most manageable adjudication method for Plaintiffs, Class Members, Defendants, and the judicial system.

488. The Class and Subclasses each satisfy the criteria for class certification under Fed. R. Civ. P. 23(b)(2).

489. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class by collecting, transmitting and storing Class Members' PII without proper data security safeguards, creating actual, imminent, and ongoing threats that Class Members will experience identity theft and fraud. The common threat to each Class Members can be mitigated by Defendants' implementation of a common set of reasonable data security protocols. An injunction mandating that Defendant implement appropriate protocols would constitute final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies and

practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge to these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class

490. Plaintiffs and the Class repeat the factual allegations alleged above as if fully set forth herein.

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

492. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

493. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs, the Nationwide Class and Subclasses.

494. Defendants owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

495. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

496. Plaintiffs and Class Members entrusted Defendants with their Private Information.

497. Plaintiffs and Class Members entrusted their Private Information to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

498. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if their Private Information were compromised or wrongfully disclosed.

499. The Data Breach was foreseeable. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and Class Members involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party. By accepting, storing, and maintaining Plaintiffs' and Class Members' Private Information, Defendants undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the Private Information of Plaintiffs and Class Members in Defendants' possession was adequately secured and protected.

500. By accepting, storing, and maintaining Plaintiffs' and Class Members' Private Information, Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to applicable laws and regulations.

501. By accepting, storing, and maintaining Plaintiffs' and Class Members' Private Information, Defendants also had a duty to implement and maintain procedures to detect and

prevent the improper access and misuse of the Private Information of Plaintiffs and Class Members.

502. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential Private Information, a necessary part of obtaining services from Defendants.

503. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or Class Members.

504. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, due to the nature of Defendants' industry, and particularly in light of Defendants' inadequate security practices.

505. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity of encrypting Private Information stored on Defendants' systems.

506. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and Class Members, including basic encryption techniques available to Defendants.

507. Defendants knew or should have known Plaintiffs' and Class Members' Private Information was stored on their database and were or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiffs' and Class Members' Private Information.

508. Despite being aware of the likelihood that Defendants' databases were vulnerable, not secure, and likely to be attacked by cybercriminals, Defendants failed to correct, update, or upgrade their security protections, thus causing the Data Breach.

509. Plaintiffs and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

510. Defendants were in the best position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

511. Defendants had and continue to have a duty to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

512. Defendants had a duty to employ proper procedures to prevent the compromise and unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

513. Defendants have admitted that the Private Information of Plaintiffs and Class Members was disclosed due to Defendants' technical security configuration issue, and thus also accessed and exfiltrated by unauthorized third persons as a result of the Data Breach.

514. Defendants improperly and inadequately safeguarded the Private Information of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

515. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and Class Members during the time the Private Information was within Defendants' possession or control.

516. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and Class Members in the face of increased risk of theft.

517. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

518. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove Private Information they were no longer required to retain pursuant to regulations.

519. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and Class Members the occurrence and scope of the Data Breach.

520. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

521. Said differently, if Defendants had properly prevented a technical security configuration issue, then the Data Breach would not have occurred, and Plaintiffs' and Class Members' Private Information would have been appropriately safeguarded.

522. Plaintiffs and Class Members suffered an injury when their Private Information was accessed by unknown third parties.

523. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, and increased risk of imminent harm, suffered by Plaintiffs and Class Members.

524. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

525. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to, the following: (i) actual fraud and identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) loss of productivity and lost opportunity costs associated with addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk and substantially increased risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate

and adequate measures to protect the Private Information of Plaintiffs and Class Members; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the loss in value of Plaintiffs' and Class Members' Private Information.

526. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

527. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which upon information and belief remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

528. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

SECOND CLAIM FOR RELIEF
NEGLIGENCE PER SE

On Behalf of Plaintiffs and the Nationwide Class

529. Plaintiffs and the Class repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

530. 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 Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

531. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by failing to comply with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they collected and stored and the foreseeable consequences and immense damages that would result to Plaintiffs and Class Members.

532. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

533. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

534. The harm resulting from the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

535. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax

fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) present and continuing costs in terms of time, effort, and money that has been and 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 Plaintiffs and Class Members.

536. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

537. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which upon information and belief remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

538. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

THIRD CLAIM FOR RELIEF
UNJUST ENRICHMENT

On Behalf of Plaintiffs and the Nationwide Class

539. Plaintiffs and the Class repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

540. To the extent the Court finds that any purported agreement fails due to an issue with contract formation, Plaintiffs plead this claim.

541. Plaintiffs and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable Private Information.

542. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

543. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members suffered as a direct and proximate result of Defendants' failure to provide the requisite data security.

544. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

545. Defendants acquired the monetary benefit and Private Information of Plaintiffs and Class Members through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

546. If Plaintiffs and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

547. Plaintiffs and Class Members have no adequate remedy at law.

548. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information 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 Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

549. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

550. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FOURTH CLAIM FOR RELIEF
BREACH OF BAILMENT

On Behalf of Plaintiffs and the Nationwide Class

551. Plaintiffs and the Class repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

552. Plaintiffs' and Class Members' Private Information is personal property.

553. Plaintiffs and Class Members provided Private Information to Defendants with the sole purpose that Defendants would use the Private Information to enter into mutually beneficial financial services contracts with Plaintiffs and Class Members.

554. Plaintiffs and Class Members provided their Private Information to Defendants on the express and implied conditions that Defendants had a duty to keep the Private Information confidential.

555. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks they took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

556. Once Defendants accepted Plaintiffs' and Class Members' Private Information, they were in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

557. Defendants did not safeguard Plaintiffs' or Class Members' Private Information when they failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

558. Defendants' failure to safeguard Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

559. As a result of Defendants' failure to keep Plaintiffs' and Class Members' Private Information secure, Plaintiffs and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—is appropriate.

FIFTH CLAIM FOR RELIEF
INVASION OF PRIVACY/INTRUSION UPON SECLUSION

On Behalf of Plaintiffs and the Nationwide Class

560. Plaintiffs and the Class repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

561. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

562. Defendants owed a duty to their customers and former customers, including Plaintiffs and Class Members, to keep their Private Information secure and confidential.

563. Defendants knew that they should keep customer Private Information confidential, as a prior consent decree and enforcement action by the Consumer Financial Protection Bureau notified Defendants of the dangers of disclosing sensitive information to third parties, and required them to cease disclosing such information to third parties.

564. Defendants' failure to implement security practices that would protect Plaintiffs' and Class Members' PII from a data breach was an intentional choice to use less costly and inferior safeguards on their computers and networks where Private Information was stored.

565. Defendants' failure to secure and protect the Private Information of Plaintiffs and Class Members from disclosure to unknown and unauthorized third parties was intentional.

566. In consciously choosing to make inferior and inadequate data security choices that failed to protect Plaintiffs' and Class Members' Private Information, Defendants allowed unauthorized and unknown third parties to access the Private Information of Plaintiffs and Class Members.

567. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person.

568. Defendants invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

569. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members entrusted their Private Information to Defendants as a prerequisite to their use of Defendants' services, but they did so privately with the intention that their Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that their Private Information would be kept private and would not be disclosed without their authorization.

570. Defendants' inadequate data security practices and the resulting Data Breach constitute intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

571. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they knew or should have known that their data security practices were inadequate and insufficient.

572. Because Defendants acted with this knowing state of mind, they had notice and knew their inadequate and insufficient data security practices would cause injury and harm to Plaintiffs and Class Members.

573. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiffs' and Class Members' privacy by:

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

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

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

574. Defendants knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendants' intentional actions highly offensive and objectionable.

575. As a proximate result of the above acts and omissions of Defendants, the Private Information of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

576. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

577. Defendants' unlawful invasions of privacy damaged Plaintiffs and Class Members. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiffs and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial and/or injunctive relief.

SIXTH CLAIM FOR RELIEF
DECLARATORY AND INJUNCTIVE RELIEF

On Behalf of Plaintiffs and the Nationwide Class

578. Plaintiffs and the Class repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

579. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

580. Defendants owe a duty of care to Plaintiffs and Class Members that require them to adequately secure Plaintiffs' and Class Members' Private Information.

581. Defendants failed to fulfill their duty of care to safeguard Plaintiffs' and Class Members' Private Information.

582. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

583. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

584. Prior consent decrees agreed upon by Defendants have not prevented their violations of the law or failure to prevent information from being disclosed to third parties.

585. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and

duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits of Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such internal security auditors;

b. Ordering that Defendants engage third-party security auditors to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for their provision of services;

e. Ordering that Defendants conduct regular database scanning and security checks; and

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Plaintiffs and Class Members' Personally Information.

SEVENTH CLAIM FOR RELIEF
Violation of O.C.G.A. § 13-6-11

On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, Georgia Plaintiffs on behalf of the Georgia Subclass

586. Plaintiffs repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

587. Defendants, through the actions alleged and described herein, acted in bad faith, were stubbornly litigious, or caused Plaintiffs and Class Members unnecessary trouble and expense with respect to the events underlying this litigation.

588. 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 companies such as Defendants for failing to implement and use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

589. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII that they obtained and stored and the foreseeable consequences of a data breach.

590. Defendants also have a duty under the Georgia Constitution ("the Constitution") which contains a Right to Privacy clause, Chapter 1, Article 1, to protect their customers' Private Information. The Georgia Constitution states, "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

591. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include the following: (i) appropriation of likeness; (ii) intrusion on solitude or seclusion; (iii) public disclosure of private facts; and (iv) false light.

592. Defendants' implementation of inadequate data security measures, their failure to resolve vulnerabilities and deficiencies, and their abdication of their responsibility to reasonably

protect data, which they required Plaintiffs and Class Members to provide and then stored on their own servers and databases, constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second) §652A.

593. Defendants knew or should have known they had a responsibility to protect the Private Information they collected from Plaintiffs and Class Members and stored, that they were entrusted with this Private Information, and that they were the only entities capable of adequately protecting the Private Information.

594. Despite that knowledge, Defendants abdicated their duty to protect the Private Information they required Plaintiffs and Class Members provide and that they stored.

595. As a direct and proximate result of Defendants' actions, Plaintiffs' and Class Members' Private Information was accessed and stolen by cybercriminals. The Data Breach was a direct consequence of Defendants' abrogation of their data security responsibilities and their decision to knowingly employ deficient data security measures that left the Private Information unsecured. Had Defendants adopted reasonable data security measures, they could have prevented the Data Breach.

596. Plaintiffs and Class Members have been injured and suffered losses directly attributable to the Data Breach.

597. Plaintiffs and Class Members therefore request that their claim for recovery of attorneys' fees and litigation expenses be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

EIGHTH CLAIM FOR RELIEF
Violations of the Georgia Uniform Deceptive Trade Practices Act
Ga. Code Ann. §§ 10-1-370, *et seq.* ("Georgia DTPA")

On Behalf of Plaintiffs and the Nationwide Class,
or, in the alternative, Georgia Plaintiffs on behalf of the Georgia Subclass

598. Plaintiffs repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

599. Defendants, Plaintiffs, and Class Members are "persons" within the meaning of the Georgia Uniform Deceptive Trade Practices Act ("Georgia DTPA"), Ga. Code Ann. § 10-1-371(5).

600. Defendants engaged in unfair and deceptive acts and practices in violation of the Georgia DTPA, Ga. Code Ann. § 10-1-372, which states in pertinent part that it is a deceptive trade practice to:

> (a)(5) Represent[] that goods or services have sponsorship, approval, characteristics, . . . uses, [or] benefits . . . that they do not have;
>
> (a)(7) Represent[] that goods or services are of a particular standard, quality, or grade . . . if they are of another; or
>
> (a)(12) Engage[] in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

601. Defendants engaged in deceptive trade practices in violation of the Georgia DTPA, Ga. Code Ann. § 10-1-372(a)(5), (7), and (12), by, among other things:

a. Omitting and concealing the material fact that they did not employ reasonable data security and privacy measures to protect consumers' Private Information. Defendants could and should have made a proper disclosure to consumers (including their customers), during their loan process, or by any other means reasonably calculated to inform consumers of the inadequate data security; and

b. Making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information. Defendants acquired consumers' Private Information during the loan process. In doing so, Defendants made implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information. By virtue of accepting Plaintiffs' and Class Members' Private Information during the loan process, Defendants implicitly represented that their data security processes were sufficient to safeguard the Private Information.

602. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

603. Because Defendants required Plaintiffs and Class Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiffs and Class Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

604. Because Defendants required Plaintiffs and Class Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiffs and Class Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

605. Plaintiffs and Class Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert

customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

606. Plaintiffs and Class Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

607. Had Defendants disclosed to Plaintiffs and Class Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information.

608. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiffs and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the loss of value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

609. To date, Defendants have not provided sufficient details regarding the full scope of the Data Breach, or any details related to the remedial measures they have taken to improve their data security practices and more fully safeguard Plaintiffs' and Class Members' Private Information from future compromise. As a result, Plaintiffs, Class Members, and Defendants' customers remain uninformed and confused as to the adequacy of Defendants' data security and Defendants' ability to protect the Private Information entrusted to them. Without adequate improvements, Plaintiffs' and Class Members' Private Information remains at an unreasonable risk of future compromise.

610. Moreover, Defendants, through their omissions and Data Breach Notice Letters, continue to represent and imply that their data security measures are adequate to protect consumers' Private Information. Such continued representations and implications, without disclosure of the full scope of the Data Breach or Defendants' subsequent remedial enhancements, place Plaintiffs and Class Members at a future risk of harm, as Plaintiffs, Class Members, and Defendants' customers are not fully informed as to whether Defendants' data security measures have been improved since the Data Breach. By all available measures, Defendants' data security practices and systems have not been adequately improved, and Plaintiffs and Class Members remain at an unreasonable risk from future cyberattacks.

611. Plaintiffs and the Class are therefore entitled to the injunctive relief sought herein, because, among other things, Defendants continue to retain their Private Information, future cyber-attacks targeting the same data are foreseeable, and Defendants have not provided sufficient notice identifying any remedial measures that will protect the data from future attack. Moreover, absent injunctive relief, Defendants will continue to misrepresent and imply that their data security practices and systems are adequate to protect the Private Information of Plaintiffs and the Class from future cyberattacks without providing any firm details or basis to support these representations.

612. The Georgia DTPA states that the "court, in its discretion, may award attorney's fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). Defendants willfully engaged in deceptive trade practices knowing them to be deceptive. Defendants knew or should have known that their data security practices were deficient. Defendants were aware that entities responsible for collecting and maintaining large amounts of

Private Information, including Social Security numbers and financial information, are frequent targets of sophisticated cyberattacks. Defendants knew or should have known that their data security practices were insufficient to guard against those attacks.

613. The Georgia DTPA states that "[c]osts shall be allowed to the prevailing party unless the court otherwise directs." Ga. Code Ann. § 10-1-373(b). Plaintiffs and the Class are entitled to recover their costs of pursuing this litigation.

614. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by the Georgia DTPA, including injunctive relief and attorneys' fees.

NINTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act of 2018
Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA")

On Behalf of Plaintiff Lana Clark and the California Subclass

615. Plaintiff Lana Clark and the California Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

616. Plaintiff Clark brings this claim individually and on behalf of the California Subclass against Defendants for violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA").

617. Defendants engaged in unfair and deceptive acts and practices in violation of the CCPA, Cal. Civ. Code § 1798.150(a)(1), which provides:

> Any consumer whose nonencrypted or nonredacted personal information, as defined in [Section 1798.81.5(d)(1)(A)], is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for [statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper].

618. Plaintiff Clark and California Subclass Members are consumers and California residents as defined by Cal. Civ. Code §1798.140(i).

619. Defendants are "business[es]" as defined by Cal. Civ. Code § 1798.140(d) because they collect and store consumers' Private Information, including sensitive and personal information as defined by Cal. Civ. Code § 1798.81.5(d)(1)(A), and have annual gross revenues in excess of $25 million. Defendants collect personal information from, among other sources, consumers who use their services to purchase consumer credit products. Defendants annually buy, receive for their commercial purposes, sell, or share for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, householders, or devices.

620. Defendants had a duty to implement and maintain reasonable data security procedures and practices to protect Plaintiff Clark's and California Subclass Members' Private Information. As a direct and proximate result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices, Plaintiff Clark's and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft and/or disclosure in violation of the CCPA, Cal. Civ. Code § 1798.150.

621. As a direct and proximate result of Defendants' failure to implement reasonable data security procedures and practices, the Private Information of approximately 4.9 million individuals, including Plaintiff Clark and the California Subclass, was accessed and stolen by unauthorized third parties. The Private Information compromised in the Data Breach included, without limitation, names, dates of birth, passport numbers, driver's license numbers, federal/state identification card numbers, tax identification numbers, Social Security numbers and/or financial account information, and other information such as phone numbers, residential addresses, and email addresses.

622. Defendants stored and maintained Plaintiff Clark's and California Subclass Members' Private Information in a form that allowed criminals to access it.

623. Defendants violated the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiff Clark's and California Subclass Members' Private Information from unauthorized access and exfiltration, theft, or disclosure.

624. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiffs and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

625. Plaintiff Clark and California Subclass Members seek relief pursuant to Cal. Civ. Code § 1798.150(a), including *inter alia*, actual damages, injunctive relief, and any other relief the Court deems proper. Plaintiff Clark and the California Subclass also seek attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

626. Because Defendants are still in possession of Plaintiff Clark's and California Subclass Members' Private Information, Plaintiff Clark and the California Subclass seek injunctive or other equitable relief to ensure that Defendants implement and maintain reasonable data security measures and practices to prevent an event like the Data Breach from occurring again.

627. Prior to filing their claims, Plaintiff Clark and the California Subclass provided prior written notice of their claims to Defendants, pursuant to Cal. Civ. Code § 1798.150(b).

Defendants have failed to cure the deficiencies that led to the Data Breach and the harm caused to Plaintiff Clark and the California Subclass. Plaintiff Clark and the California Subclass therefore seek all actual and compensatory damages according to proof or statutory damages allowable under the CCPA, whichever are higher, and such other and further relief as this Court may deem just and proper, including injunctive or declaratory relief.

TENTH CLAIM FOR RELIEF
Violation of the California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq.* ("CLRA")

On Behalf of Plaintiff Lana Clark and the California Subclass

628. Plaintiff Lana Clark and the California Subclass repeat the factual allegations alleged above as if fully set forth herein.

629. Plaintiff Clark brings this claim individually and on behalf of the California Subclass against Defendants for violation of the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.* ("CLRA"), which is liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property, or services to consumers for personal, family, or household use.

630. Defendants are "person[s]" that provided "services" pursuant to the CLRA, Cal. Civ. Code §§ 1761(b)-(c), 1770.

631. Plaintiff Clark and California Subclass Members are "consumer[s]" who engaged in "transaction[s]" with Defendants, as defined under the CLRA, Cal. Civ. Code §§ 1761(d)-(e), 1770.

632. Defendants engaged in unfair and deceptive acts and practices in violation of the CLRA, Cal. Civ. Code § 1770, which prohibits companies, like Defendants, from:

> (a)(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."
>
> (a)(7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (a)(14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or that are prohibited by law.

633. Defendants' acts and practices were intended to and did result in the sale of services to Plaintiff Clark and California Subclass Members in violation of the CLRA, Cal. Civ. Code § 1770(a)(5), (7) and (14), by, among other things, omitting and concealing the material fact that Defendants did not implement and maintain adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information.

634. Defendants' deceptive, unfair, and unlawful acts or practices in violation of the CLRA include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Clark's and California Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Clark's and California Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Clark's and California Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Clark's and California Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Clark's and California Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

635. Defendants' omissions and misrepresentations were material because they were likely to and did deceive reasonable consumers, including Plaintiff Clark and California Subclass Members, about the adequacy of Defendants' data security practices and their ability to protect the confidentiality of the Private Information they solicited, collected, stored, and maintained.

636. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff Clark's and California Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

637. Because Defendants required Plaintiff Clark and California Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Clark and California Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

638. Because Defendants required Plaintiff Clark and California Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Clark and California Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

639. Plaintiff Clark and California Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

640. Plaintiff Clark and California Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

641. Had Defendants disclosed to Plaintiff Clark and California Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

642. Instead, Defendants solicited, collected, stored, and maintained Plaintiff Clark's and California Subclass Members' Private Information, as part of the services Defendants provided and for which Plaintiff Clark and California Subclass Members paid, by omitting and concealing information from Plaintiff Clark and California Subclass Members that (1) Defendants' data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiff Clark's and California Subclass Members' Private Information and (2) Defendants were not compliant with basic data security requirements and industry best practices. Accordingly, Plaintiff Clark and California Subclass Members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered.

643. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiff Clark and California Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

644. Prior to filing their claims, Plaintiff Clark and the California Subclass provided prior written notice of their claims for damages to Defendants, in compliance with Cal. Civ. Code § 1782(a). Defendants have failed to cure the deficiencies that led to the Data Breach and the harm caused to Plaintiff Clark and the California Subclass.

645. Plaintiff Clark and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

ELEVENTH CLAIM FOR RELIEF
Violation of the Wisconsin Deceptive Trade Practices Act
Wis. Stat. Ann. § 100.18 ("Wisconsin DTPA")

On Behalf of Plaintiffs Ryan Carder, Sophia Pickens, Joseph Trottier, and the Wisconsin Subclass

646. Plaintiffs Ryan Carder, Sophia Pickens, Joseph Trottier, and the Wisconsin Subclass repeat the factual allegations alleged above as if fully set forth herein.

647. Plaintiffs Carder, Pickens and Trottier bring this claim individually and on behalf of the Wisconsin Subclass against Defendants for violation of the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18(1) ("Wisconsin DTPA"), which prohibits untrue, deceptive, or misleading representations in the sale of goods and services to consumers.

648. Defendants are "corporation[s] or association[s]," as defined by the Wisconsin DTPA, Wis. Stat. § 100.18(1).

649. Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members are members of "the public," as defined by the Wisconsin DTPA, Wis. Stat. § 100.18(1).

650. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Defendants to members of the public for sale, use, or distribution, Defendants made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of the Wisconsin DTPA, Wis. Stat. § 100.18(1).

651. Defendants also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of the Wisconsin DTPA, Wis. Stat. § 100.18(9).

652. Defendants' deceptive acts, practices, plans, and schemes in violation of the Wisconsin DTPA include:

a. Implementing inadequate data security and privacy measures to protect the Private Information of Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of the Private Information of Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure the Private Information of Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

653. Defendants intended to mislead Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members and induce them to rely on their misrepresentations and omissions.

654. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

655. Defendants had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity of the Private Information in their possession, and the generally accepted professional standards in the financial services industry. This duty arose because members of the public, including Plaintiffs Carder, Pickens, Trottier, and the Wisconsin Subclass, repose a trust and confidence in Defendants as their loan servicer. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs Carder, Pickens, Trottier, and the Wisconsin Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the inadequate security of the data in their systems;

b. Active concealment of the inadequate condition of their data security; and/or

c. Incomplete representations about the security and integrity of their computer and data systems.

656. Because the above facts are material to a reasonable person in Plaintiffs' position, the law treats Defendants' failure to disclose them as being identical to actively representing that those facts do not exist.

657. Defendants acted intentionally, knowingly, and maliciously to violate the Wisconsin DTPA, and recklessly disregarded the rights of Plaintiffs Carder, Pickens, Trottier, and the Wisconsin Subclass.

658. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members have suffered and will continue to suffer ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; a substantially increased and imminent risk of fraud and identity theft; loss of value of their Private Information, and the need to dedicate future expenses and time to protect themselves against further loss.

659. Defendants had an ongoing duty to all their customers to refrain from deceptive acts, practices, plans, and schemes under the Wisconsin DTPA, Wis. Stat. § 100.18.

660. Plaintiffs Carder, Pickens, Trottier, and Wisconsin Subclass Members seek all monetary and nonmonetary relief allowed by law, including damages, reasonable attorneys' fees, and costs of suit under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

TWELFTH CLAIM FOR RELIEF
Violation of the Virginia Consumer Protection Act
Va. Code Ann. §§ 59.1-196, *et seq.* ("VCPA")

On Behalf of Plaintiffs Sheneequa Carrington, Jeremiah Gills, Ebony Millner, and the Virginia Subclass

661. Plaintiffs Sheneequa Carrington, Jeremiah Gills, Ebony Millner, and the Virginia Subclass repeat the factual allegations alleged above as if fully set forth herein.

662. Plaintiffs Carrington, Gills, and Millner bring this claim individually and on behalf of the Virginia Subclass against Defendants for violation of the Virginia Consumer Protection Act of 1977, Va. Code Ann. §§ 59.1-196, *et seq.* ("VCPA"), which is designed "to promote fair and ethical standards of dealings between suppliers and the consuming public." Va. Code Ann. § 59.1-197.

663. The VCPA prohibits "fraudulent acts or practices committed by a supplier in connection with a consumer transaction[,]" including: "[m]isrepresenting that goods or services are of a particular standard, quality, grade, style, or model." Va. Code Ann. § 59.1-200(6).

664. Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members are "[p]erson[s]" and Defendants are "supplier[s]" within the meaning of the VCPA, Va. Code Ann. §59.1-198.

665. Defendants engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by the VCPA, Va. Code Ann. § 59.1-198, because Defendants advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

666. Defendants engaged in deceptive acts and practices in violation of the VCPA by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Implementing inadequate data security and privacy measures to protect the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure and protect the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

667. Defendants intended to mislead Plaintiffs Carrington, Gills, Millner, and the Virginia Subclass and induce them to rely on their misrepresentations and omissions.

668. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members, about the adequacy of Defendants' computer and data security and the quality of the Defendants' brand.

669. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiffs' and Virginia Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

670. Because Defendants required Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiffs and Virginia Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

671. Because Defendants required Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

672. Plaintiffs Carrington, Gills, Millner, and Virginia Sublass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security,

including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

673. Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

674. Had Defendants disclosed to Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members that their data security practices, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members would not have entrusted Defendants with their Private Information, Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

675. Instead, Defendants solicited, received, stored, maintained, and compiled the Private Information of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members as part of the services Defendants provided, without advising Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of their Private Information. Accordingly, Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

676. Defendants had a duty to disclose these material facts concerning the inadequacies of their data security practices, due to the circumstances of this case and the sensitivity of the Private Information in their possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers and Defendants, because consumers

are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the security of the data in their systems;

b. Active concealment of the state of their security; and/or

c. Incomplete representations about the security and integrity of their computer and data systems, while purposefully withholding material facts from Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members that contradicted these representations.

677. The above-described deceptive acts and practices also violated the following provisions of the VCPA, Va. Code Ann. § 59.1-200:

> (A)(5) Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;
>
> (A)(6) Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and
>
> (A)(8) Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

678. Defendants acted intentionally, knowingly, and maliciously to violate the VCPA, Va. Code Ann. §§ 59.1-200(A)(5), (6) and (8), and recklessly disregarded the rights of Plaintiffs Carrington, Gills, Millner, and Virginia Subclass Members.

679. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiffs Carrington, Gills, Millner, and the Virginia Subclass suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent

and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

680. Defendants' violations present a continuing risk to Plaintiffs Carrington, Gills, Millner, and the Virginia Subclass as well as to the general public.

681. Plaintiffs Carrington, Gills, Millner, and the Virginia Subclass seek all monetary and nonmonetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

THIRTEENTH CLAIM FOR RELIEF
Violation of Alabama Deceptive Trade Practices Act Ala. Code §§ 8-19-1, *et seq.* ("Alabama DTPA")

On Behalf of Plaintiffs Adrian Johnson, Lakendra Mitchell, and the Alabama Subclass

682. Plaintiffs Adrian Johnson, Lakendra Mitchell, and the Alabama Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

683. Plaintiffs Johnson and Mitchell bring this claim, individually and on behalf of the Alabama Subclass, against Defendants for violation of the Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1, *et seq.* ("Alabama DTPA").

684. Plaintiffs Johnson, Mitchell, and Alabama Subclass Members are "consumer[s]" within the meaning of the Alabama DTPA, Ala. Code § 8-19-3(5).

685. Defendants' loan services are "services" within the meaning of the Alabama DTPA, Ala. Code § 8- 19-3(13).

686. Defendants were and are engaged in "trade or commerce" within the meaning of the Alabama DTPA, Ala. Code § 8-19-3(14).

687. The Alabama DTPA declares several specific actions to be unlawful, including: "Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce." Ala. Code § 8-19-5(27).

688. Defendants participated in unfair or deceptive trade practices that violated the Alabama DTPA, including:

a. Implementing inadequate data security and privacy measures to protect the Private Information of Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of the Private Information of Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure the Private Information of Plaintiffs Johnson, Mitchell, and Alabama Subclass Members; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

689. Defendants intended to mislead Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, and induce them to rely on their misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiffs Johnson, Mitchell, and Alabama Subclass Members, about the adequacy of Defendants' computer and data security and the quality of Defendants' brand.

690. Defendants knew or should have known their conduct violated the Alabama DTPA.

691. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiffs' and Alabama Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

692. Because Defendants required Plaintiffs Johnson, Mitchell, and Alabama Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiffs Johnson, Mitchell, and Alabama Subclass Members reasonably expected that

Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

693. Because Defendants required Plaintiffs Johnson, Mitchell, and Alabama Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiffs Johnson, Mitchell, and Alabama Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

694. Plaintiffs Johnson, Mitchell, and Alabama Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

695. Plaintiffs Johnson, Mitchell, and Alabama Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions of material facts regarding their data security practices.

696. Had Defendants disclosed to Plaintiffs Johnson, Mitchell, and Alabama Sublass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

697. Had Plaintiffs Johnson, Mitchell, and Alabama Subclass Members known that as a result of utilizing Defendants' services, their Private Information would be revealed to hackers or other third parties, Plaintiffs Johnson, Mitchell, and the Alabama Subclass would not have

utilized Defendants' services or would have paid less for them. Plaintiffs Johnson, Mitchell, and the Alabama Subclass did not receive the benefit of their bargain as a result of Defendants' misconduct.

698. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiffs Johnson, Mitchell, and the Alabama Subclass suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

699. Plaintiffs Johnson, Mitchell, and the Alabama Subclass seek an order enjoining Defendants' unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Alabama DTPA.

FOURTEENTH CLAIM FOR RELIEF
Violations of Illinois Consumer Fraud and Deceptive Business Practices Act 815 Ill. Comp. Stat. §§ 505, *et seq.* ("Illinois CPA")

On Behalf of Plaintiff Edwin Scheide and the Illinois Subclass

700. Plaintiff Edwin Scheide and the Illinois Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

701. Plaintiff Scheide brings this claim, individually and on behalf of the Illinois Subclass, against Defendants for violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505, *et seq.* ("Illinois CPA").

702. Defendants are "person[s]" as defined by the Illinois CPA, 815 Ill. Comp. Stat. § 505/1(c).

703. Plaintiff Scheide and Illinois Subclass Members are "consumer[s]" as defined by the Illinois CPA, 815 Ill. Comp. Stat. § 505/1(e).

704. Defendants' complained-of conduct as described herein was in "trade" or "commerce" as defined by the Illinois CPA, 815 Ill. Comp. Stat. § 505/1(f).

705. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of the Illinois CPA, 815 Ill. Comp. Stat. § 505/2, including by:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Scheide's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade

Commission Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Scheide's and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

706. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Scheide and Illinois Subclass Members, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

707. Defendants intended to mislead Plaintiff Scheide and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

708. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff Scheide's and Illinois Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

709. Because Defendants required Plaintiff Scheide and Illinois Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Scheide and Illinois Subclass Members reasonably expected that Defendants' data security,

digital platforms, and data storage systems were adequately secure to protect their Private Information.

710. Because Defendants required Plaintiff Scheide and Illinois Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Scheide and Illinois Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

711. Plaintiff Scheide and Illinois Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

712. Plaintiff Scheide and Illinois Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

713. Had Defendants disclosed to Plaintiff Scheide and Illinois Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

714. Defendants acted intentionally, knowingly, and maliciously to violate the Illinois CPA, and recklessly disregarded Plaintiff Scheide's and Illinois Subclass Members' rights.

715. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiff Scheide and Illinois Subclass Members suffered ascertainable losses,

including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

716. Plaintiff Scheide and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

FIFTEENTH CLAIM FOR RELIEF
Violations of Illinois Uniform Deceptive Trade Practices Act
815 Ill. Comp. Stat. §§ 510, *et seq.* ("Illinois DTPA")

On Behalf of Plaintiff Edwin Scheide and the Illinois Subclass

717. Plaintiff Edwin Scheide and the Illinois Subclass repeat the factual allegations alleged above as if fully set forth herein.

718. Plaintiff Scheide brings this claim, individually and on behalf of the Illinois Subclass, against Defendants for violations of the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. §§ 510, *et seq.* ("Illinois DTPA").

719. Defendants are "person[s]" as defined by the Illinois DTPA, 815 Ill. Comp. Stat. § 510/1(5).

720. Defendants engaged in deceptive trade practices in the conduct of their business, in violation of the Illinois DTPA, 815 Ill. Comp. Stat. §§ 510/2, which prohibits companies like Defendants from:

> (a)(5) Representing that goods or services have characteristics that they do not have;

> (a)(7) Representing that goods or services are of a particular standard, quality, or grade if they are of another;
>
> (a)(9) Advertising goods or services with intent not to sell them as advertised; and
>
> (a)(12) Engaging in any other conduct that creates a likelihood of confusion or misunderstanding.

721. Defendants engaged in unfair and deceptive acts and practices in violation of the Illinois DTPA, 815 Ill. Comp. Stat. §§ 510/2(a)(5), (7), (9) and (12), by, among other things, omitting and concealing the material fact that Defendants did not implement and maintain adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information.

722. Defendants' deceptive, unfair, and unlawful acts or practices in violation of the Illinois DTPA include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Scheide's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Scheide's and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scheide's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

723. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Scheide and Illinois Subclass Members, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

724. Defendants intended to mislead Plaintiff Scheide and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

725. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff Scheide's and Illinois Subclass

Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

726. Because Defendants required Plaintiff Scheide and Illinois Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Scheide and Illinois Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

727. Because Defendants required Plaintiff Scheide and Illinois Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Scheide and Illinois Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

728. Plaintiff Scheide and Illinois Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

729. Plaintiff Scheide and Illinois Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

730. Had Defendants disclosed to Plaintiff Scheide and Illinois Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private

Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

731. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiff Scheide and Illinois Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

732. Plaintiff Scheide and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

SIXTEENTH CLAIM FOR RELIEF
Violations of Florida Deceptive and Unfair Trade Practices Act Fla. Stat. § 501.201, *et seq.* ("FDUTPA")

On Behalf of Plaintiff Amy Penird and the Florida Subclass

733. Plaintiff Amy Penird and the Florida Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

734. Plaintiff Penird brings this claim, individually and on behalf of the Florida Subclass, against Defendants for violations of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.* ("FDUTPA").

735. Defendants engaged in unfair or deceptive acts or practices in the conduct of their trade or commerce, in violation of the FDUTPA, Fla. Stat. § 501.204, by, among other things, omitting and concealing the material fact that Defendants did not implement and maintain

adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information.

736. Defendants' deceptive, unfair, and unlawful acts or practices in violation of the FDUTPA include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Penird's and Florida Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Penird's and Florida Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Penird's and Florida Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Penird's and Florida Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Penird's and Florida Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Penird's and Florida Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

737. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Penird and Florida Subclass Members, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

738. Defendants intended to mislead Plaintiff Penird and Florida Subclass Members and induce them to rely on their misrepresentations and omissions.

739. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff Penird's and Florida Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

740. Because Defendants required Plaintiff Penird and Florida Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Penird and Florida Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

741. Because Defendants required Plaintiff Penird and Florida Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff

Penird and Florida Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

742. Plaintiff Penird and Florida Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

743. Plaintiff Penird and Florida Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

744. Had Defendants disclosed to Plaintiff Penird and Florida Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

745. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiff Penird and Florida Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

746. Plaintiff Penird and the Florida Subclass seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

SEVENTEENTH CLAIM FOR RELIEF
Violation of Missouri Merchandising Practices Act
Mo. Stat. § 407.010, et seq. ("MMPA")

On Behalf of Plaintiff LaPetra Robinson and the Missouri Subclass

747. Plaintiff LaPetra Robinson and the Missouri Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

748. Plaintiff Robinson brings this claim, individually and on behalf of the Missouri Subclass, against Defendants for violation of the Missouri Merchandising Practices Act, Mo. Stat. § 407.010, *et seq.* ("MMPA").

749. Defendants are "person[s]" as defined by the MMPA, Mo. Stat. § 407.010(5).

750. Defendants' loan services are "merchandise" within the meaning of the MMPA, Mo. Stat. § 407.010(4).

751. Defendants were and are engaged in "trade or commerce" within the meaning of the MMPA, Mo. Stat. § 407.010(7).

752. The MMPA declares several specific actions to be unlawful, including "[t]he act use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Stat. § 407.020(1).

753. Defendants participated in unfair or deceptive trade practices that violated the MMPA, including:

a. Implementing inadequate data security and privacy measures to protect the Private Information of Plaintiff Robinson and Missouri Subclass Members, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff Robinson and Missouri Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of the Private Information of Plaintiff Robinson and Missouri Subclass Members, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff Robinson and Missouri Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure the Private Information of Plaintiff Robinson and Missouri Subclass Members; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the

Private Information of Plaintiff Robinson and Missouri Subclass Members, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

754. Defendants intended to mislead Plaintiff Robinson and Missouri Subclass Members, and induce them to rely on their misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Robinson and Missouri Subclass Members, about the adequacy of Defendants' computer and data security and the quality of Defendants' brand.

755. Defendants knew or should have known their conduct violated the MMPA.

756. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff Robinson and Missouri Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

757. Because Defendants required Plaintiff Robinson and Missouri Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Robinson and Missouri Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

758. Because Defendants required Plaintiff Robinson and Missouri Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Robinson and Missouri Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

759. Plaintiff Robinson and Missouri Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

760. Plaintiff Robinson and Missouri Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions of material facts regarding their data security practices.

761. Had Defendants disclosed to Plaintiff Robinson and Missouri Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

762. Had Plaintiff Robinson and Missouri Subclass Members known that as a result of utilizing Defendants' services, their Private Information would be revealed to hackers or other third parties, Plaintiff Robinson and Missouri Subclass Members would not have utilized Defendants' services or would have paid less for them. Plaintiff Robinson and Missouri Subclass Members did not receive the benefit of their bargain as a result of Defendants' misconduct.

763. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiff Robinson and Missouri Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially

increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

764. Plaintiff Robinson and Missouri Subclass Members seek an order enjoining Defendants' unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the MMPA.

EIGHTEENTH CLAIM FOR RELIEF
Violation of Tennessee Consumer Protection Act
Tenn. Code Ann. § 47-18-101, et seq. ("TCPA")

On Behalf of Plaintiff Adam White and the Tennessee Subclass

765. Plaintiff Adam White and the Tennessee Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

766. Plaintiff White brings this claim, individually and on behalf of the Tennessee Subclass, against Defendants for violation of the Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-101, *et seq.* ("TCPA").

767. Plaintiff White and Tennessee Subclass members are "consumers" as defined by the TCPA, Tenn. Code Ann. § 47-18-103(6).

768. Defendants are "person[s]" as defined by the TCPA, Tenn. Code Ann. § 47-18-103(18).

769. Defendants were and are engaged in "trade or commerce" within the meaning of the TCPA, Tenn. Code Ann. § 47-18-103(24).

770. Defendants engaged in deceptive trade practices in the conduct of their business, in violation of the TCPA, Tenn. Code Ann. § 47-18-104, which prohibits persons like Defendants from:

> (b)(5) Representing that goods or services have characteristics, benefits, or qualities that they do not have;

> (b)(7) Representing that goods or services are of a particular standard, quality, or grade if they are of another;
>
> (b)(9) Advertising goods or services with intent not to sell them as advertised; and
>
> (b)(27) Engaging in any other act or practice which is deceptive to the consumer.

771. Defendants engaged in unfair and deceptive acts and practices in violation of the TCPA, Tenn. Code Ann. § 47-18-104(b)(5), (7), (9), and (27) by, among other things, omitting and concealing the material fact that Defendants did not implement and maintain adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information.

772. Defendants' deceptive, unfair, and unlawful acts or practices in violation of the TCPA include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff White's and Tennessee Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff White's and Tennessee Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff White's and Tennessee Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff White's and Tennessee Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff White's and Tennessee Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff White's and Tennessee Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

773. Defendants intended to mislead Plaintiff White and Tennessee Subclass Members, and induce them to rely on their misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff White and Tennessee Subclass Members, about the adequacy of Defendants' computer and data security and the quality of Defendants' brand.

774. Defendants knew or should have known their conduct violated the TCPA.

775. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff White and Tennessee Subclass

Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

776. Because Defendants required Plaintiff White and Tennessee Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff White and Tennessee Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

777. Because Defendants required Plaintiff White and Tennessee Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff White and Tennessee Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

778. Plaintiff White and Tennessee Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

779. Plaintiff White and Tennessee Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions of material facts regarding their data security practices.

780. Had Defendants disclosed to Plaintiff White and Tennessee Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private

Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

781. Had Plaintiff White and Tennessee Subclass Members known that as a result of utilizing Defendants' services, their Private Information would be revealed to hackers or other third parties, Plaintiff White and Tennessee Subclass Members would not have utilized Defendants' services or would have paid less for them. Plaintiff White and Tennessee Subclass Members did not receive the benefit of their bargain as a result of Defendants' misconduct.

782. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiff White and Tennessee Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

783. Plaintiff White and Tennessee Subclass Members seek an order enjoining Defendants' unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the TCPA.

NINTEENTH CLAIM FOR RELIEF
Violation of Nevada Deceptive Trade Practices Act
Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.* ("Nevada DTPA")

On Behalf of Plaintiff Melvin Nicholas and the Nevada Subclass

784. Plaintiff Melvin Nicholas and the Nevada Subclass repeat the factual allegations alleged above in paragraphs 1 through 489 as if fully set forth herein.

785. Plaintiff Nicholas brings this claim, individually and on behalf of the Nevada Subclass, against Defendants for violation of the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.* ("Nevada DTPA").

786. Defendants are "person[s]" within the meaning of the Nevada DTPA.

787. Defendants' high-interest loans are "goods or services" within the meaning of the Nevada DTPA.

788. Defendants engaged in unfair or deceptive acts or practices in the conduct of their trade or commerce, in violation of the Nevada DTPA, by, among other things, omitting and concealing the material fact that Defendants did not implement and maintain adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that their data security practices were sufficient to protect consumers' Private Information.

789. Defendants engaged in deceptive trade practices in the conduct of their business, in violation of the Nevada DTPA, Nev. Rev. Stat. Ann. §§ 598.0915 and 598.0923, which prohibits persons like Defendants from:

> § 598.0915(5) Knowingly making a false representation as to the characteristics or benefits of goods or services for sale;
>
> § 598.0915(7) Representing that goods or services are of a particular standard, quality, or grade if the person knows or should know that they are of another;
>
> § 598.0915(9) Advertising goods or services with intent not to sell them as advertised;
>
> § 598.0915(15) Knowingly making a false representation in a transaction;
>
> § 598.0923(1)(b) Failing to disclose a material fact in connection with the sale of goods or services; and

§ 598.0923(1)(c) Violating a state or federal statute or regulation relating to the sale of goods or services.

790. Defendants' deceptive, unfair, and unlawful acts or practices in violation of the Nevada DTPA include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Nicholas's and Nevada Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Nicholas's and Nevada Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45 and Nev. Rev. Stat. Ann. §§ 603A.210, 603A.215, and 603A.220;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Nicholas's and Nevada Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Nicholas's and Nevada Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45 and Nev. Rev. Stat. Ann. §§ 603A.210, 603A.215, and 603A.220;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Nicholas's and Nevada Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Nicholas's and Nevada Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45 and Nev. Rev. Stat. Ann. §§ 603A.210, 603A.215, and 603A.220.

791. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Nicholas and Nevada Subclass Members, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

792. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Nicholas and Nevada Subclass Members, about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

793. Defendants knew that their data security practices were inadequate and intended to mislead Plaintiff Nicholas and Nevada Members and induce them to rely on their misrepresentations and omissions.

794. Past breaches in the financial services industry put Defendants on notice that their data security practices were inadequate to safeguard Plaintiff Nicholas's and Nevada Subclass Members' Private Information, and Defendants knew or should have known that the risk of a data breach was highly likely.

795. Because Defendants required Plaintiff Nicholas and Nevada Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Wright and South Carolina Subclass Members reasonably expected that Defendants' data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

796. Because Defendants required Plaintiff Nicholas and Nevada Subclass Members to provide their Private Information as a prerequisite to their use of Defendants' services, Plaintiff Nicholas and Nevada Subclass Members relied on Defendants to advise customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

797. Plaintiff Nicholas and Nevada Subclass Members had no opportunity to make any inspection of Defendants' data security practices or to otherwise ascertain the truthfulness of Defendants' representations and omissions regarding data security, including Defendants' failure to alert customers that their data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

798. Plaintiff Nicholas and Nevada Subclass Members relied to their detriment on Defendants' misrepresentations and deceptive omissions regarding their data security practices.

799. Had Defendants disclosed to Plaintiff Nicholas and Nevada Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs would not have entrusted Defendants with their Private Information, and Defendants would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

800. As a direct and proximate result of Defendants' unfair and deceptive business practices, Plaintiff Nicholas and Nevada Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the loss of value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

801. Plaintiff Nicholas and Nevada Subclass seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. Certify this case as a Class Action pursuant to Federal Rule of Civil Procedure 23;

B. Order appropriate compensatory, injunctive, equitable, declaratory, punitive, and nominal relief to Plaintiffs and Class Members under the applicable law;

C. Award Plaintiffs an appropriate Class Representative Service Award for their prosecution of this matter on behalf of all Class Members;

D. Award Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

E. Award reasonable attorneys' fees and costs in accordance with O.C.G.A. § 13-6-11 and as permitted by law; and

F. Enter other and further such relief as the Court deems to be both just and fair.

DEMAND FOR JURY TRIAL

A jury trial is demanded on all claims so triable.

Date: November 29, 2023

Respectfully submitted,

/s/ Thomas A. Withers
Thomas A. Withers
Georgia Bar No. 772250
Withers Law Firm, P.C.
8 East Liberty Street
Savannah, GA 31401
Tel. 912.447.8400
twithers@witherslawfirmpc.com

Interim Liaison Counsel

MaryBeth V. Gibson
Georgia Bar No. 725843
The Finley Firm, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, Georgia 30305
Tel. 404.320.9979
mgibson@thefinleyfirm.com

Kelly Iverson
Pro Hac Vice
Lynch Carpenter, LLP
1133 Penn Avenue
5th Floor
Pittsburg, Pennsylvania 15222
Tel. 412.322.9243
kelly@lcllp.com

Amy Keller
Pro Hac Vice
DiCello Levitt LLP
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dicellolevitt.com

Interim Co-Lead Counsel

Rebecca Franklin Harris
Franklin Law, LLC
2250 East Victory Drive
Suite 102
Savannah, Georgia 31404
Tel. 912.335.3305
rebecca@franklinlawllc.com

Interim Chair, Plaintiffs' Steering Committee

James J. Pizzirusso
Pro Hac Vice
Hausfeld LLP
888 16th Street, NW
Suite 300
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Carl Malmstrom
Pro Hac Vice
Wolf Haldenstein Adler Freeman & Herz LLP
111 W. Jackson Blvd.
Suite 1700
Chicago, Illinois 60604
Tel. 312.984.0000
malmstrom@whafh.com

Terry Coates
Markovits, Stock & DeMarco, LLC
119 East Court Street
Suite 530
Cincinnati, Ohio 45202
Tel. 513.651.3700
tcoates@msdlegal.com

William B. Federman
Federman & Sherwood
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
Tel. 405.235.1560
wbf@federmanlaw.com

Brian C. Gudmundson
Pro Hac Vice
Zimmerman Reed LLP
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Tel. 612.341.0400
brian.gudmundson@zimmreed.com

Interim Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I, Thomas A. Withers, hereby certify that I filed a copy of the foregoing using this Court's CM/ECF service, which will send notification of such filing to all counsel of record this 29th day of November, 2023.

/s/ Thomas A. Withers
Thomas A. Withers

Interim Plaintiffs' Liaison Counsel