ROBINSON CALCAGNIE, INC.
Daniel S. Robinson (SBN 244245)
drobinson@robinsonfirm.com
Michael W. Olson (SBN 312857)
molson@robinsonfirm.com
19 Corporate Plaza Drive
Newport Beach, California
(949) 720-1288; Fax: (949) 720-1292

AHDOOT & WOLFSON, PC
Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Alyssa Brown (SBN 301313)
abrown@ahdootwolfson.com
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
(310) 474-9111; Fax: (310) 474-8585

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
(800) 400-6808; Fax: (800) 520-5523

LARSON LLP
Stephen G. Larson (SBN 145225)
slarson@larsonllp.com
555 S. Flower Street, 30th Floor
Los Angeles, CA 90071
(213) 436-4864; Fax: (213) 623-2000

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Gary M. Klinger (*Pro Hac Pending*)
gklinger@milberg.com
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
(866) 252-0878

Interim Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, SOUTHERN DIVISION

In re loanDepot Data Breach Litigation	Case No. 8:24-cv-00136-DOC-JDEx
	Assigned For All Purposes to Courtroom 10A: Hon. David O. Carter
This Document Relates to: All Cases	**CONSOLIDATED CLASS ACTION COMPLAINT**
	DEMAND FOR JURY TRIAL

Plaintiffs Alphonso Woods, David Ware, Deborah McPhail, Josh Krieghauser, Daroya Isaiah, Joshua Beller, Maurice Beckwith, Robert Lash, Ryan Azinger, Lorenz Praefcke, Varun Singh, Debra Coe, Loretta Montgomery, Vidal Hernandez, Tracy Brown, Branislav Sasic, Jessica Schuler, Kyle Nunnelly, Nailah Ricco-Brown, and Matthew McFall, individually and on behalf of all others similarly situated, (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint and allege the following against Defendant loanDepot, Inc. ("loanDepot" or "Defendant"), based upon personal knowledge as to their own acts and investigations, the investigation of counsel, and information and belief.

I. INTRODUCTION

1. This case is about loanDepot's failure to adequately secure and safeguard its vulnerable networks, resulting in a massive data breach where the personally identifiable information of approximately 16.9 million[1] of its nationwide customers was allegedly accessed and exfiltrated by unauthorized parties. According to loanDepot's announcement made on or around January 8, 2024, between January 3-5, 2024, an unauthorized third party gained access to loanDepot's systems, including certain sensitive personal information stored in those systems (the "Data Breach"). The personal information included Plaintiffs' and putative class members' names, addresses, email addresses, financial account numbers, Social Security numbers ("SSN"), phone numbers, and dates of birth (collectively, "Private Information").

2. As a result of Defendant's failure to implement expected and industry-standard data security practices, Plaintiffs and members of the proposed classes (defined below) (collectively, the "Class Members") suffered foreseeable, preventable, and ascertainable losses.

//

[1] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/2b910ff6-9bd0-4fcf-a766-cd2c0bc85dec.shtml (last visited May 9, 2024).

3. loanDepot is an Irvine, California-based nonbank holding company and the nation's fifth largest retail mortgage lender, funding more than 27,000 consumer mortgages per month.[2]

4. loanDepot was on notice that it was vulnerable to a cyberattack. Not only is it industry-wide knowledge that financial institutions experience a consistent stream of cyberattacks, but loanDepot itself just recently suffered a similar data breach that exposed its customers' Private Information. In August 2022, third parties hacked into loanDepot's inadequately secured systems and stole thousands of customers' Private Information. In that instance, nine months passed until loanDepot even notified its customers that their Private Information had been stolen, including names and other personal identifiers in combination with SSNs.[3] Despite knowing of its susceptibility to a targeted cyberattack and knowing the consequences that would result to consumers, loanDepot turned a blind eye, failing to implement adequate safeguards to protect its customers' confidential Private Information.

5. On January 8, 2024, loanDepot announced that once again data thieves had targeted and gained unauthorized access to its systems and compromised the Private Information of approximately 16.6 million individuals.[4] That same day, loanDepot reported in its mandatory U.S. Securities and Exchange Commission ("SEC") disclosure that hackers had breached its systems.[5]

6. Because of the severity of the Data Breach at issue, on or about January

[2] *About Us,* loanDepot, https://loandepot.com/about (last visited May 1, 2024).
[3] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/60385809-5ea7-44e0-93a5-4ee98fb42e1e.shtml (last visited May 9, 2024).
[4] *loanDepot Provides Update on Cyber Incident,* loanDepot (Jan. 22, 2024), https://investors.loandepot.com/news/corporate-and-financial-news/corporate-and-financial-news-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last visited June 3, 2024).
[5] *See* loanDepot Form 8-K Filing, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/446c437f-153f-425d-adc6-bf37155d6e91.pdf (last visited May 30, 2024).

8, 2024, loanDepot shut down its website, including its customer portals.[6]

7. loanDepot's customer service portal, "mellohomes.com" website, HELOC customer portal, and "myloandepot" customer portal were all down and inaccessible until January 18, 2024.

8. Considering the severity of the Data Breach, the steps that loanDepot has taken have been insufficient and perfunctory.

9. After keeping its customers largely in the dark for two weeks, on January 22, 2024, loanDepot issued the following press release regarding the Data Breach:

> loanDepot, Inc. ("LDI" or "Company") (NYSE: LDI), a leading provider of home lending solutions, today provided an update on the cyber incident it disclosed on January 8, 2024. The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible . . . . Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to the sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.[7]

10. The January 22, 2024 "update" provided little new information, other than informing customers they were eligible for free credit monitoring services. This offer for free services is both the minimum loanDepot could offer in light of the magnitude of harm it has caused, and serves as a tacit acknowledgment of the detrimental and elevated risk that all Class Members now imminently face as a result of Defendant's acts and omissions surrounding the Data Breach.

11. In this update, Defendant's CEO Frank Martel acknowledged: "we live in a world where these types of attacks are increasingly frequent and sophisticated,

---

[6] Zack Whittaker, *LoanDepot hit by suspected ransomware attack*, TECHCRUNCH (Jan. 8, 2024, 10:00 a.m. PST), https://techcrunch.com/2024/01/08/loandepot-outage-suspected-ransomware-attack/ (last visited June 3, 2024).

[7] *See*, *supra*, n. 4.

and our industry has not been spared. We sincerely regret any impact on our customers."[8] This message was nothing more than an attempt to deflect responsibility for loanDepot's failure to fulfill its legal obligations to protect Plaintiffs' and Class Members' Private Information. The frequency of these types of attacks is exactly why loanDepot should have taken greater steps to protect Private Information.

12. On or about February 23, 2024, almost six weeks after the initial January 8 announcement and SEC filing, Defendant began to provide notice of the Data Breach to its past, present, or prospective customers, employees, and state attorneys general.[9] Through these reportings, loanDepot revealed that the number of individuals affected by this massive Data Breach grew to 16,924,071.

13. Through its notice, loanDepot provided that, "[a]s discussed further below, we recommend you remain vigilant with respect to reviewing your account statements and credit reports." loanDepot also provided "Steps You May Take to Protect Yourself Against Potential Misuse of Information," which includes reviewing account statements and periodically pulling a credit report, reviewing fraud alerts, and obtaining a credit freeze, among other steps that loanDepot recommends Plaintiffs and Class Members take following the Data Breach.

14. Thus, even loanDepot acknowledges the risks associated with the Data Breach, and that Plaintiffs and Class Members should take immediate steps to protect themselves from potential harm. loanDepot is, therefore, estopped from contending Plaintiffs' and Class Members' protective actions were unnecessary, unwise, or unwarranted.

15. Despite the threat actors (the ALPHV/BlackCat ransomware gang) publicly identifying themselves and claiming credit for the Data Breach on February

[8] *See*, *supra*, n. 4.

[9] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/2b910ff6-9bd0-4fcf-a766-cd2c0bc85dec.shtml (last visited June 3, 2024).

16, 2024, Defendant did not begin to send notices to Plaintiffs, customers, employees, and states' attorneys general for another week.[10] The notice did not include critical information that the threat actors provided, including that the Russian-linked ransomware gang wrote, "Your information is in the final process of being sold. That's all."[11] Defendant has failed to provide sufficient details surrounding the Data Breach to enable breach victims to arm themselves against fraud and identity theft.

16. loanDepot's failure to implement adequate safeguards is particularly troublesome considering its assurances that it would safeguard its customers' confidential information. Indeed, loanDepot warrants to consumers that it has "adopted policies and procedures designed to protect [their] personally identifiable information" and that "all data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility."[12]

17. Relying on these assurances, Plaintiffs and Class Members shared and entrusted their Private Information with loanDepot, its officials, and its agents with the understanding that—at a minimum—loanDepot would take reasonable steps to ensure that this information remained private, safe, and secure from breaches and attacks.

18. Up to and through January 2024, loanDepot collected, maintained, and stored Class Members' Private Information in an unsecured, unencrypted, and

[10] Stefanie Schappert, *LoanDepot finally reveals what data was exposed in Jan hack,* Cybernews (Feb. 26, 2024, 9:21 p.m.), https://cybernews.com/news/loandepot-finally-reveals-what-data-exposed-in-jan-hack/.

[11] *Id*.

[12] *Privacy Policy*, loanDepot, https://www.loandepot.com/privacypolicy (last visited May 30, 2024).

internet-accessible environment, from which unauthorized actors used an extraction tool to retrieve sensitive Private Information belonging to Plaintiffs and millions of Class Members.

19. Despite loanDepot's knowledge that its systems were vulnerable to cyberattacks and its assurances to its customers that it would adequately safeguard Private Information, Defendant knowingly and willfully maintained Private Information in a grossly negligent and/or reckless manner by storing that sensitive information in a condition vulnerable to cyberattacks.

20. The severe consequences of exposing Plaintiffs and Class Members' Private Information to data thieves cannot be exaggerated. Private Information is such a valuable commodity to identity-thieves that once the information has been compromised, it is circulated and traded by criminals on the "cyber black-market" for years.[13] Indeed, as noted above, on February 16, 2024, the threat actors here publicly announced that the stolen data was in the final process of being sold.[14]

21. As a result of the Data Breach and Defendant's untimely notice, Plaintiffs and Class Members have been exposed to a present, heightened, and imminent risk of fraud and identity theft. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, but not limited to, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' email and telephone information to target Class Members for other phishing and hacking intrusions, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class

[13] *PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* U.S. Government Accountability Office, GAO-07-737 (June 2007), at p. 29, https://www.gao.gov/new.items/d07737.pdf.

[14] *See*, *supra*, n. 10.

Members' information, obtaining driver's licenses in Class Members' names, and more.

22. Because of Defendant's willful conduct, Plaintiffs and Class Members have been required and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their Private Information, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, reviewing and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate records. This time will be lost forever and cannot be recaptured.

23. Plaintiffs bring this class action on behalf and as representatives of all similarly situated persons whose personal information was compromised by the Data Breach. Plaintiffs seek damages and declaratory and injunctive relief to remediate loanDepot's inadequate data security procedures and practices.

II. PARTIES

A. Plaintiffs

Josh Krieghauser

24. Plaintiff Josh Krieghauser is a resident and citizen of Descanso, California. Mr. Krieghauser is a customer of loanDepot and applied for and/or obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot required Mr. Krieghauser to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Krieghauser received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Krieghauser reasonably expected

loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Krieghauser reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Krieghauser known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

25. Mr. Krieghauser is careful about sharing his sensitive Private Information. Mr. Krieghauser first learned of the Data Breach after receiving a data breach notification letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Krieghauser made reasonable efforts to mitigate the impact thereof, including, but not limited to, purchasing an identity theft prevention service and frequently monitoring his various accounts. In the time following the Data Breach, Mr. Krieghauser has experienced a significant increase in spam phone calls. Mr. Krieghauser has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Krieghauser suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Krieghauser has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

26. Mr. Krieghauser has a continuing interest in ensuring that his Private

Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Krieghauser because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Varun Singh

27. Plaintiff Varun Singh is a resident and citizen of Newark, California. Mr. Singh is a customer of loanDepot and applied for and/or obtained a loan from loanDepot in or around November 17, 2020. As a condition of applying for the loan, loanDepot required Mr. Singh to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Singh received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Singh reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Singh reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Singh known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

28. Mr. Singh is careful about sharing his sensitive Private Information. Mr. Singh first learned of the Data Breach after receiving a data breach notification letter in March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information, including his social security number, had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr.

Singh made reasonable efforts to mitigate the impact thereof, including, but not limited to, placing a credit freeze and resetting passwords to his various accounts. In the time following the Data Breach, Mr. Singh has experienced unauthorized attempts to access his accounts, and he has received calls from anonymous numbers trying to open accounts using his social security number. Mr. Singh has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Singh suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Singh has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

29. Mr. Singh has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Singh because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Daroya Isaiah

30. Plaintiff Daroya Isaiah is a resident and citizen of Adelanto, California. Ms. Isaiah was a customer of loanDepot and applied for and/or obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot required Ms. Isaiah to provide her Private Information to loanDepot in order to utilize its services. Prior to applying for the loan, Ms. Isaiah received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which she reviewed and relied on prior to providing her

Private Information to loanDepot. In providing her Private Information to loanDepot, Ms. Isaiah reasonably expected loanDepot would maintain the privacy and security of her Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Ms. Isaiah reasonably understood that a portion of the funds that she would have paid to loanDepot would be used to pay for adequate data security and protection of her Private Information. Had Ms. Isaiah known about loanDepot's inadequate data security, she would not have provided her Private Information to loanDepot.

31. Ms. Isaiah is careful about sharing her sensitive Private Information. Ms. Isaiah first learned of the Data Breach after receiving a data breach notification letter from loanDepot, notifying her of the Data Breach and that her Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Ms. Isaiah made reasonable efforts to mitigate the impact thereof, including, but not limited to, spending time monitoring her various accounts, disputing unauthorized charges, freezing her credit, and purchasing credit reports. In the time following the Data Breach, Ms. Isaiah has experienced unauthorized fraudulent charges, including an unauthorized fraudulent attempt to receive governmental student aid in her name. Ms. Isaiah has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because loanDepot disclosed her Private Information to unauthorized parties who may now use that information for unknown purposes, and any unauthorized activity could have affected her approval during the homebuying process. Ms. Isaiah suffered actual injuries in the form of damages to and diminution in the value of her Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Ms. Isaiah has suffered and will continue to suffer for the remainder of her life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized

third parties and/or cybercriminals.

32. Ms. Isaiah has a continuing interest in ensuring that her Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Ms. Isaiah because it prevented her from having the earliest opportunity to guard herself against the Data Breach's harmful effects and she would have sooner been able to seek a mortgage loan through another service provider at a better interest rate.

Alphonso Woods

33. Plaintiff Alphonso Woods is a resident and citizen of Valley Grande, Alabama. Alphonso Woods is a customer of loanDepot and applied for and/or obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot required Mr. Woods to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Woods received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Woods reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Woods reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Woods known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

34. Mr. Woods is careful about sharing his sensitive Private Information. Mr. Woods first learned of the Data Breach after receiving a data breach notification letter

dated February 2024, from loanDepot, notifying him of the Data Breach and that his Private Information, including Social Security Number, had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Woods made reasonable efforts to mitigate the impact thereof, including, but not limited to, freezing his credit and signing up for a monitoring service. In the time following the Data Breach, Mr. Woods has experienced a significant increase in spam calls, texts, and emails. Mr. Woods has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Woods suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Woods has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

35. Mr. Woods has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Woods because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

David Ware

36. Plaintiff David Ware is a resident and citizen of Phoenix, Arizona. Mr. Ware is a customer of loanDepot and applied for and/or obtained a loan from loanDepot on or around June 2021. As a condition of applying for the loan, loanDepot required Mr. Ware to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Ware received and

reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Ware reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Ware reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Ware known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

37. Mr. Ware is careful about sharing his sensitive Private Information. Mr. Ware first learned of the Data Breach after receiving a data breach notification letter in or around March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Ware made reasonable efforts to mitigate the impact thereof, including, but not limited to, subscribing to an identity theft prevention service and frequently monitoring his online accounts. In the time following the Data Breach, Mr. Ware has experienced a number of suspicious emails and unknown individuals opened unauthorized phone accounts using his information. Mr. Ware has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Ware suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Ware has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

38. Mr. Ware has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Ware because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Deborah McPhail

39. Plaintiff Deborah McPhail is a resident and citizen of Raymond, Maine. Ms. McPhail is a customer of loanDepot and applied for and/or obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot required Ms. McPhail to provide her Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Ms. McPhail received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which she reviewed and relied on prior to providing her Private Information to loanDepot. In providing her Private Information to loanDepot, Ms. McPhail reasonably expected loanDepot would maintain the privacy and security of her Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Ms. McPhail reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of her Private Information. Had Ms. McPhail known about loanDepot's inadequate data security, she would not have provided her Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

//

40. Ms. McPhail is careful about sharing her sensitive Private Information. Ms. McPhail first learned of the Data Breach after receiving a data breach notification letter from loanDepot, notifying her of the Data Breach and that her Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Ms. McPhail made reasonable efforts to mitigate the impact thereof, including, but not limited to, purchasing identity theft protection and spending time monitoring her various accounts. In the time following the Data Breach, Ms. McPhail has experienced an increase in spam phone calls. Ms. McPhail has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed her Private Information to unauthorized parties who may now use that information for unknown purposes. Ms. McPhail suffered actual injuries in the form of damages to and diminution in the value of her Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Ms. McPhail has suffered and will continue to suffer for the remainder of her life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and/or cybercriminals.

41. Ms. McPhail has a continuing interest in ensuring that her Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Ms. McPhail because it prevented her from having the earliest opportunity to guard herself against the Data Breach's harmful effects.

Joshua Beller

42. Plaintiff Joshua Beller is a resident and citizen of Commerce City, Colorado. Mr. Beller is a customer of loanDepot and applied for and/or obtained a loan from loanDepot in or around August 2020. As a condition of applying for the

loan, loanDepot required Mr. Beller to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Beller received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Beller reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Beller reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Beller known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

43. Mr. Beller is careful about sharing his sensitive Private Information. Mr. Beller first learned of the Data Breach after receiving a data breach notification letter in or around March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Beller made reasonable efforts to mitigate the impact thereof, including, but not limited to, purchasing an identity theft prevention service and spending hours a week monitoring his various online accounts. In the time following the Data Breach, Mr. Beller has experienced a significant uptick in spam calls and spam emails. Mr. Beller has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Beller suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach.

Mr. Beller has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

44. Mr. Beller has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Beller because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Maurice Beckwith

45. Plaintiff Maurice Beckwith is a resident and citizen of Durham, North Carolina. Mr. Beckwith is a customer of loanDepot and applied for and/or obtained a loan from loanDepot. As a condition of applying for the loan, loanDepot required Mr. Beckwith to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Beckwith received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Beckwith reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Beckwith reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Beckwith known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

46. Mr. Beckwith is careful about sharing his sensitive Private Information. Mr. Beckwith first learned of the Data Breach after receiving a data breach notification letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Beckwith made reasonable efforts to mitigate the impact thereof, including, but not limited to, obtaining credit monitoring services and freezing his credit. In the time following the Data Breach, Mr. Beckwith has experienced fraudulent charges, unauthorized credit cards opened in his name, and an increase in spam calls, texts, and emails. Mr. Beckwith has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Beckwith suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Beckwith has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

47. Mr. Beckwith has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Beckwith because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Robert Lash

48. Plaintiff Robert Lash is a resident and citizen of Montague, Michigan. Mr. Lash is a customer of loanDepot and applied for and/or obtained a loan from

loanDepot around ten years ago. As a condition of applying for the loan, loanDepot required Mr. Lash to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Lash received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Lash reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Lash reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Lash known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

49. Mr. Lash is careful about sharing his sensitive Private Information. Mr. Lash first learned of the Data Breach after receiving a data breach notification letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Lash made reasonable efforts to mitigate the impact thereof, including, but not limited to, signing up for an identity theft prevention service and freezing his credit. In the time following the Data Breach, Mr. Lash has experienced attempted fraudulent charges on his bank account and an increase in spam calls. Mr. Lash has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Lash suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which

was compromised in and as a proximate result of the Data Breach. Mr. Lash has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

50. Mr. Lash has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Lash because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Ryan Azinger

51. Plaintiff Ryan Azinger is a resident and citizen of Sudbury, Massachusetts. Mr. Azinger is a customer of loanDepot and applied for and/or obtained a loan from loanDepot on or around June 2021. As a condition of applying for the loan, loanDepot required Mr. Azinger to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Azinger received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Azinger reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Azinger reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Azinger known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a

mortgage loan through another service provider.

52. Mr. Azinger is careful about sharing his sensitive Private Information. Mr. Azinger first learned of the Data Breach after receiving a data breach notification letter in or around late March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Azinger made reasonable efforts to mitigate the impact thereof, including, but not limited to, freezing his credit and informing his local financial institutions about the compromised data. In the time following the Data Breach, Mr. Azinger has experienced a number of incidents where someone attempted to open credit accounts in his name. Mr. Azinger has already received notifications that his information was on the dark web. Mr. Azinger has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Azinger suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Azinger has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

53. Mr. Azinger has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Azinger because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

//

Lorenz Praefcke

54. Plaintiff Lorenz Praefcke is a resident and citizen of Berwyn, Pennsylvania. Mr. Praefcke is a customer of loanDepot and applied for and/or obtained a loan from loanDepot on or around June 2021. As a condition of applying for the loan, loanDepot required Mr. Praefcke to provide his Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Mr. Praefcke received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which he reviewed and relied on prior to providing his Private Information to loanDepot. In providing his Private Information to loanDepot, Mr. Praefcke reasonably expected loanDepot would maintain the privacy and security of his Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Mr. Praefcke reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of his Private Information. Had Mr. Praefcke known about loanDepot's inadequate data security, he would not have provided his Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

55. Mr. Praefcke is careful about sharing his sensitive Private Information. Mr. Praefcke first learned of the Data Breach after receiving a data breach notification letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Mr. Praefcke made reasonable efforts to mitigate the impact thereof, including, but not limited to, having multiple conversations with Chase, securing his account, talking to his bank to decline additional applications, and freezing his credit with Transunion. In the time following the Data Breach, but before receiving the notice, Mr. Praefcke experienced two unauthorized attempts to open credit cards in his name, along with a significant

number of spam calls and emails. Mr. Praefcke has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information to unauthorized parties who may now use that information for unknown purposes. Mr. Praefcke suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Praefcke has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

56. Mr. Praefcke has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Praefcke because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Debra Coe

57. Plaintiff Debra Coe is a resident and citizen of Northbrook, Illinois. Ms. Coe is a customer of loanDepot and applied for and/or obtained a loan from loanDepot in or around 2019. As a condition of applying for the loan, loanDepot required Ms. Coe to provide her Private Information to loanDepot in order to utilize its services. Prior to applying for and/or securing the loan, Ms. Coe received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which she reviewed and relied on prior to providing her Private Information to loanDepot. In providing her Private Information to loanDepot, Ms. Coe reasonably expected loanDepot would maintain the privacy and security of her Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

Ms. Coe reasonably understood that a portion of the funds paid to loanDepot would be used to pay for adequate data security and protection of her Private Information. Had Ms. Coe known about loanDepot's inadequate data security, she would not have provided her Private Information to loanDepot and/or would have applied for and/or obtained a mortgage loan through another service provider.

58. Ms. Coe is careful about sharing her sensitive Private Information. Ms. Coe first learned of the Data Breach after receiving a data breach notification letter dated February 2024, from loanDepot, notifying her of the Data Breach and that her Private Information, including her social security number, had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Ms. Coe made reasonable efforts to mitigate the impact thereof. In the time following the Data Breach, Ms. Coe has experienced a significant increase in spam calls and texts. Ms. Coe has also experienced fear, stress, and frustration because loanDepot disclosed her Private Information to unauthorized parties who may now use that information for unknown purposes. Ms. Coe suffered actual injuries in the form of damages to and diminution in the value of her PII—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Ms. Coe has suffered and will continue to suffer for the remainder of her life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and/or cybercriminals.

59. Ms. Coe has a continuing interest in ensuring that her Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Ms. Coe because it prevented her from having the earliest opportunity to guard herself against the Data Breach's harmful effects.

//

Nailah Ricco-Brown

60. Plaintiff Nailah Ricco-Brown is a resident and citizen of New York, New York. Ms. Ricco-Brown was a customer of loanDepot and applied for a loan from loanDepot as part of a program in conjunction with the State of New York Mortgage Agency. As a condition of applying for the loan, loanDepot required Ms. Ricco-Brown to provide her Private Information to loanDepot in order to utilize its services. Prior to applying for the loan, Ms. Ricco-Brown received and reviewed a contract and other documents from loanDepot, which included and/or incorporated by reference loanDepot's Privacy Policy, which she reviewed and relied on prior to providing her Private Information to loanDepot. In providing her Private Information to loanDepot, Ms. Ricco-Brown reasonably expected loanDepot would maintain the privacy and security of her Private Information, and would use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law. Ms. Ricco-Brown reasonably understood that a portion of the funds that she would have paid to loanDepot would be used to pay for adequate data security and protection of her Private Information. Had Ms. Ricco-Brown known about loanDepot's inadequate data security, she would not have provided her Private Information to loanDepot. Upon learning of the Data Breach, she discontinued her applications process with loanDepot, which delayed her mortgage loan, resulting in her obtaining a mortgage loan through another service provider at a higher interest rate than she would have otherwise received.

61. Ms. Ricco-Brown is careful about sharing her sensitive Private Information. Ms. Ricco-Brown first learned of the Data Breach after receiving a data breach notification letter from loanDepot, notifying her of the Data Breach and that her Private Information had been improperly accessed and acquired by unauthorized third parties. Upon receiving notice of the Data Breach, Ms. Ricco-Brown made reasonable efforts to mitigate the impact thereof, including, but not limited to, spending time monitoring her various accounts and continuing to pay for credit

monitoring. In the time following the Data Breach, Ms. Ricco-Brown has experienced an increase in spam phone calls and messages, and she received a notification that someone had sought a personal loan through a lender in her name for which she did not seek. Ms. Ricco-Brown has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because loanDepot disclosed her Private Information to unauthorized parties who may now use that information for unknown purposes, and any unauthorized activity could have affected her approval during the homebuying process. Ms. Ricco-Brown suffered actual injuries in the form of damages to and diminution in the value of her Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Ms. Ricco-Brown has suffered and will continue to suffer for the remainder of her life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and/or cybercriminals.

62. Ms. Ricco-Brown has a continuing interest in ensuring that her Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Ms. Ricco-Brown because it prevented her from having the earliest opportunity to guard herself against the Data Breach's harmful effects and she would have sooner been able to seek a mortgage loan through another service provider at a better interest rate.

Loretta Montgomery

63. Plaintiff Loretta Montgomery is a resident and citizen of Fremont, Ohio. Ms. Montgomery does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer, and does not know or recall how loanDepot obtained her Private Information. Had Ms. Montgomery known that loanDepot possessed her Private Information, she would have expected

loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

64. Ms. Montgomery is careful about sharing her sensitive Private Information. Ms. Montgomery first learned of the Data Breach after receiving a data breach notification letter dated February 23, 2024, from loanDepot, notifying her of the Data Breach and that her Private Information, including her social security number, had been improperly accessed and acquired by unauthorized third parties. Although she has never been a loanDepot customer and did not know loanDepot possessed her Private Information, Ms. Montgomery still took the notice seriously, and made reasonable efforts to mitigate the impact thereof. In the time following the Data Breach, Ms. Montgomery has experienced an increase in spam calls. Ms. Montgomery has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed her Private Information, which she does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Ms. Montgomery suffered actual injuries in the form of damages to and diminution in the value of her Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Ms. Montgomery has suffered and will continue to suffer for the remainder of her life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and/or cybercriminals.

65. Ms. Montgomery has a continuing interest in ensuring that her Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Ms. Montgomery because it prevented her from having the earliest opportunity to guard herself against the Data Breach's harmful effects.

Vidal Hernandez

66. Plaintiff Vidal Hernandez is a resident and citizen of Brooklyn, New York. Mr. Hernandez does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer, and does not know or recall how loanDepot obtained his Private Information. Had Mr. Hernandez known that loanDepot possessed his Private Information, he would have expected loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

67. Mr. Hernandez is careful about sharing his sensitive Private Information. Mr. Hernandez first learned of the Data Breach after receiving a data breach notification letter in or around March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information, including his social security number, had been improperly accessed and acquired by unauthorized third parties. Although he has never been a loanDepot customer and did not know loanDepot possessed his Private Information, Mr. Hernandez still took the notice seriously, and made reasonable efforts to mitigate the impact thereof. In the time following the Data Breach, Mr. Hernandez has experienced an increase in spam calls, as well as unauthorized charges on his debit card. Mr. Hernandez has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information, which he does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Mr. Hernandez suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Hernandez has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

68. Mr. Hernandez has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Hernandez because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Tracy Brown

69. Plaintiff Tracy Brown is a resident and citizen of West Memphis, Arkansas. Mr. Brown does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer, and does not know or recall how loanDepot obtained his Private Information. Had Mr. Brown known that loanDepot possessed his Private Information, he would have expected loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

70. Mr. Brown is careful about sharing his sensitive Private Information. Mr. Brown first learned of the Data Breach after receiving a data breach notification letter, from loanDepot, notifying him of the Data Breach and that his Private Information, including his social security number, had been improperly accessed and acquired by unauthorized third parties. Although he has never been a loanDepot customer and did not know loanDepot possessed his Private Information, Mr. Brown still took the notice seriously, and made reasonable efforts to mitigate the impact thereof, including, but not limited to, purchasing an identity theft prevention service and freezing his credit. In the time following the Data Breach, Mr. Brown has experienced an increase in spam calls. Mr. Brown has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information, which he does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Mr. Brown suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of

intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Brown has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

71. Mr. Brown has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Brown because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Branislav Sasic

72. Plaintiff Branislav Sasic is a resident and citizen of Frisco, Texas. Mr. Sasic does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer, and does not know or recall how loanDepot obtained his Private Information. Had Mr. Sasic known that loanDepot possessed his Private Information, he would have expected loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

73. Mr. Sasic is careful about sharing his sensitive Private Information. Mr. Sasic first learned of the Data Breach after receiving a data breach notification letter in or around March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information had been improperly accessed and acquired by unauthorized third parties. Although he has never been a loanDepot customer and did not know loanDepot possessed his Private Information, Mr. Sasic still took the notice seriously, and made reasonable efforts to mitigate the impact thereof. In the time following the Data Breach, Mr. Sasic has experienced an issue when renewing his auto and

homeowner insurance policy, resulting in an almost $2,000 increase in premium due to a "no hit" on his credit. Mr. Sasic has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information, which he does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Mr. Sasic suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Sasic has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

74. Mr. Sasic has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Sasic because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Jessica Schuler

75. Plaintiff Jessica Schuler is a resident and citizen of Gainesville, Florida. Ms. Schuler does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer. Had Ms. Schuler known that loanDepot possessed her Private Information, she would have expected loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

76. Ms. Schuler is careful about sharing her sensitive Private Information. Ms. Schuler first learned of the Data Breach after receiving a data breach notification letter in or around March 2024, from loanDepot, notifying her of the Data Breach and

that her Private Information, including her social security number, had been improperly accessed and acquired by unauthorized third parties. Although she has never been a loanDepot customer and did not know loanDepot possessed her Private Information, Ms. Schuler still took the notice seriously, and made reasonable efforts to mitigate the impact thereof, including, but not limited to, purchasing an identity theft prevention service and freezing her credit. In the time following the Data Breach, Ms. Schuler has experienced an increase in spam phone calls, emails, and spam text messages. Ms. Schuler has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed her Private Information, which she does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Ms. Schuler suffered actual injuries in the form of damages to and diminution in the value of her Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Ms. Schuler has suffered and will continue to suffer for the remainder of her life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and/or cybercriminals.

77. Ms. Schuler has a continuing interest in ensuring that her Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Ms. Schuler because it prevented her from having the earliest opportunity to guard herself against the Data Breach's harmful effects.

Kyle Nunnelly

78. Plaintiff Kyle Nunnelly is a resident and citizen of Westland, Michigan. Mr. Nunnelly does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer, and does not know or recall how loanDepot obtained his Private Information. Had Mr. Nunnelly known

that loanDepot possessed his Private Information, he would have expected loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

79. Mr. Nunnelly is careful about sharing his sensitive Private Information. Mr. Nunnelly first learned of the Data Breach after receiving a data breach notification letter in or around March 2024, from loanDepot, notifying him of the Data Breach and that his Private Information, including his social security number, had been improperly accessed and acquired by unauthorized third parties. Although he has never been a loanDepot customer and did not know loanDepot possessed his Private Information, Mr. Nunnelly still took the notice seriously, and made reasonable efforts to mitigate the impact thereof, including, but not limited to, purchasing an identity theft prevention service and placing a freeze on his credit with all three credit bureaus. In the time following the Data Breach, Mr. Nunnelly has experienced an increase in spam calls. Mr. Nunnelly has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information, which he does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Mr. Nunnelly suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. Nunnelly has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

80. Mr. Nunnelly has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. Nunnelly because it

prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

Matthew McFall

81. Plaintiff Matthew McFall is a resident and citizen of Downers Grove, Illinois. Mr. McFall does not recall having applied for a loan or refinance through loanDepot, or otherwise recall having been a loanDepot customer, and does not know or recall how loanDepot obtained his Private Information. Had Mr. McFall known that loanDepot possessed his Private Information, he would have expected loanDepot to use reasonable measures to protect it in accordance with loanDepot's internal policies, as well as state and federal law.

82. Mr. McFall is careful about sharing his sensitive Private Information. Mr. McFall first learned of the Data Breach after receiving a data breach notification letter dated February 23, 2024, from loanDepot, notifying him of the Data Breach and that his Private Information, including his social security number, had been improperly accessed and acquired by unauthorized third parties. Although he has never been a loanDepot customer and did not know loanDepot possessed his Private Information, Mr. McFall still took the notice seriously and made reasonable efforts to mitigate the impact thereof. In the time following the Data Breach, Mr. McFall has experienced an increase in spam calls and text messages and an unauthorized attempt to change the name on his mortgage. Mr. McFall has and is additionally experiencing fear, stress, and frustration because loanDepot disclosed his Private Information, which he does not recall providing to loanDepot, to unauthorized parties who may now use that information for unknown purposes. Mr. McFall suffered actual injuries in the form of damages to and diminution in the value of his Private Information—a form of intangible property entrusted to loanDepot, which was compromised in and as a proximate result of the Data Breach. Mr. McFall has suffered and will continue to suffer for the remainder of his life imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting

from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

83. Mr. McFall has a continuing interest in ensuring that his Private Information, which remains within loanDepot's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks. The delayed notification provided by loanDepot further impacted Mr. McFall because it prevented him from having the earliest opportunity to guard himself against the Data Breach's harmful effects.

B. Defendant

84. loanDepot is an Irvine, California-based nonbank company that sells mortgage and non-mortgage lending products. loanDepot is a corporation formed in Delaware and registered in California, with a principal place of business located at 6561 Irvine Center Drive, Irvine, California.

III. JURISDICTION AND VENUE

85. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), as amended by the Class Action Fairness Act of 2005, because (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class Members; (3) at least one Class Member is diverse from Defendant; and (4) the Defendant is not a government entity.

86. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and in this District through its headquarters, offices, parents, and affiliates.

87. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

//

IV. FACTS

A. loanDepot Collects, Stores, and Maintains Substantial Amounts of Private Information, Which it Ensured it Would Safeguard

88. loanDepot is a California-based retail mortgage lender and nonbank holding company. It is the country's fifth-largest retail mortgage lender and the second largest nonbank retail originator. Since its founding in 2010, Defendant has provided more than $275 billion in lending. loanDepot currently employs more than 6,000 individuals and services more than 27,000 customers each month.[15]

89. To utilize loanDepot's services, customers are required to provide loanDepot with a large quantity of highly sensitive and private information; loanDepot collects and maintains its customer's Private Information in its computer systems, servers, and networks. On its privacy policy webpage, loanDepot admits to collecting the following confidential and sensitive consumer Private Information[16]:

Information We Collect

Consumer and Customers

We collect information about you to help us serve your financial, real estate, insurance, credit, and homeownership-related needs; to provide you with quality products and services; and to fulfill legal and regulatory requirements. We consider non-public information about you in our possession to be personally identifiable information, even if you cease to be a customer. The personally identifiable information we collect about you may include:

- Identifying information, such as your name, age, address, phone number and social security number
- Employment information
- Contact information (such as first and last name, mailing or property address, phone number, email address)
- Account access information, such as username and password
- Demographic information (such as date of birth, gender, marital status, ethnicity, race)
- Social security, driver's license, passport, and other government identification numbers
- Loan account information (such as loan number)
- Bank account and credit/debit card numbers
- Other personal information needed from you to provide real estate-related, loan-related, insurance-related, credit-related, and homeownership-related services to you
- Information for fraud detection and prevention
- Financial information such as your income, assets and liabilities, as well as information about your savings, investments, insurance and business.

[15] *See*, *supra*, n. 2.
[16] *Supra*, n. 12.

90. Defendant is and was aware of the sensitive nature of the Private Information it collects, and the importance of safeguarding it.

91. In fact, Defendant acknowledged the significant risks of collecting and maintaining Private Information. In Defendant's Privacy Policy, it advanced a litany of assurances and promises to its customers that it will maintain the security and privacy of their personal information[17]:

Safeguarding Personally Identifiable Information

- We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.
- We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.
- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.
- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing or developing our products or services.
- Our policy, which governs the conduct of all of our employees, requires all employees to safeguard personally identifiable information about the consumers and customers we serve or have served in the past.

loanDepot Security Policy

loanDepot takes steps to safeguard your personal and sensitive information through industry standard physical, electronic, and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.

92. Defendant made numerous promises to Plaintiffs and Class Members that they would maintain the security and privacy of their Private Information. For instance, in its Privacy Policy, Defendant assures consumers that while it shares customers' Private Information with third parties "as required or permitted by law," Defendant's "policy is to require third-party service providers to enter into confidentiality agreements with [loanDepot], prohibiting them from using any personally identifiable information they obtain for any other purpose other than those

[17] *Id.*

for which they were retained or as required by law."[18]

93. Defendant provided each of its applicants and customers with a copy of its Privacy Policy and other policies and required each customer to sign an acknowledgment of the terms thereof. Based on further information and belief, loanDepot was otherwise bound by the representations made in these agreements, regardless of whether Plaintiffs and/or Class Members executed an acknowledgment, by its acceptance of Plaintiffs' and Class Members' Private Information.

94. Through these policies, among others, loanDepot made promises to Plaintiffs and Class Members that it would protect their Private Information by maintaining adequate data security, acknowledged that it was a predictable target of unauthorized parties for a data breach, such as the Data Breach, and led Plaintiffs and Class Members to believe loanDepot could be trusted with their Private Information. By failing to protect Plaintiffs' and Class members' Private Information, by allowing the Data Breach to occur, and otherwise disclosing Plaintiffs' and Class Members' Private Information, Defendant broke these privacy promises.

95. Plaintiffs and Class Members took reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained.

96. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal, equitable, and affirmative duties to safeguard their Private Information.

97. Plaintiffs and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business purposes, and to prevent the unauthorized disclosure of Private Information.

//

[18] *Id.*

98. Despite these extensive proclaimed proactive policies and approaches to maintain data security and privacy for its customers, loanDepot failed to adequately safeguard its systems and networks from a foreseeable and preventable cyberattack. This conduct proximately caused the Data Breach and significant, irreparable harm to Plaintiffs and Class Members.

B. The Data Breach: loanDepot Failed to Safeguard Valuable Consumer Private Information

99. On or around January 8, 2024, loanDepot posted the following online:

> loanDepot is experiencing a cyber incident.
>
> We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers and we are focused on resolving these matters as soon as possible.[19]

100. Following the breach, Defendant intermittently posted updates to its website alerting customers when its various subsidiaries' payment portals were reactivated. On or about January 22, 2024, Defendant posted the following statement in response to the Data Breach:

> The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyloanDepot and Servicing customer portals.
>
> Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.

[19] *loanDepot is experiencing a cyber incident*, loanDepot, https://loandepot.cyberincidentupdate.com/ (last visited May 30, 2024).

> "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact on our customers," said loanDepot CEO Frank Martell. "The entire loanDepot team has worked tirelessly throughout this incident to support our customers, our partners and each other. I am pleased by our progress in quickly bringing our systems back online and restoring normal business operations."
> "Our customers are at the center of everything we do," said Jeff Walsh, President of loanDepot Mortgage. "I'm really proud of our team, and we're glad to be back to doing what we do best: enabling our customers across the country to achieve their financial goals and dreams of homeownership."
>
> The Company is committed to keeping its customers, partners, and employees informed and will provide any additional operational updates on our microsite at loandepot.cyberincidentupdate.com.[20]

101. Although loanDepot claimed to be working to restore "normal" operations, there was no acknowledgment that the insufficiency of "normal" operations led to the Data Breach in the first place. loanDepot did not express any desire to change, update, or otherwise improve security and other protocols which clearly failed here, let alone provide any clear explanation of what new security protocols and safeguards it will put in place.

//

//

//

//

//

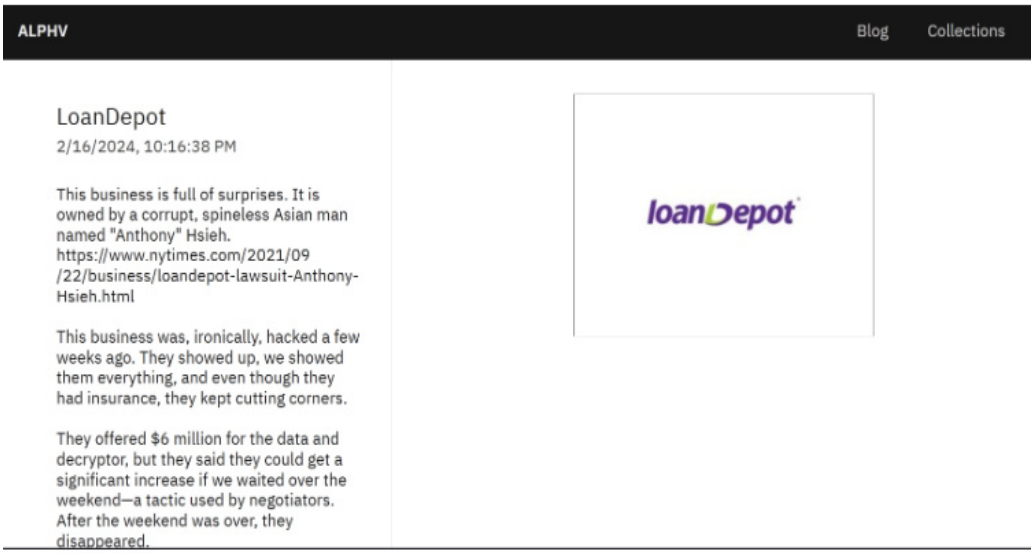
//

//

//

[20] *Supra*, n. 4.

102. On February 16, 2024, the ALPHV/BlackCat ransomware gang publicly identified themselves and claimed credit for the Data Breach. ALPHV/BlackCat named the home lender on its leak blog on February 16th, accompanied by a lengthy post singling out the company for "cutting corners" and failing to pay a ransom[21]:



103. In ALPHV's post, it also called out the online mortgage firm for not disclosing "the full amount of data stolen." The group stated: "We downloaded multiple databases from credit bureaus that included personal information about American citizens, even those who had never applied for any of their products From [*sic*] their accesses." Furthermore, ALPHV claims loanDepot "withheld information about 4 TB of additional data that included comprehensive client data."[22]

104. The threat actors also provided considerable information about loanDepot's failure to pay the ransom. The gang blamed the so-called failed ransom negotiations on the company's legal team, insurance underwriters, and being "unable to make up their minds." "They offered $6 million for the data and decryptor… we waited over the weekend—a tactic used by negotiators. After the weekend was over, they disappeared," ALPHV wrote.[23]

[21] *See*, *supra*, n. 10.
[22] *Id.*
[23] *Id.*

105. Additionally, the gang implied it had sources at the company feeding them inside information. "The CIO [Chief Information Officer] was 10 steps behind us and was feeding the Executive team false information on purpose. Our insiders at this company informed us that they were being pressured to leave [the negotiations] by their outside counsel," the post said. "As their networks were being taken over, they took weeks to make a decision… and finally turned to leave" ALPHV added.[24]

106. Due to the failed negotiations over a ransom, the threat actors monetized the stolen data by selling it, writing "Your information is in the final process of being sold. That's all . . . ."[25]

107. ALPHV/BlackCat is a well-known threat actor that first appeared in 2021. Known for its triple-extortion tactics, the gang was responsible for the September 2023 ransomware attacks on the Las Vegas casino giants MGM Resorts and Caesars International. ALPHV/BlackCat is a known threat that Defendant chose to ignore.

108. True to their word, ALPHV/BlackCat had posted loanDepot's data on their website:

//

//

//

//

//

//

//

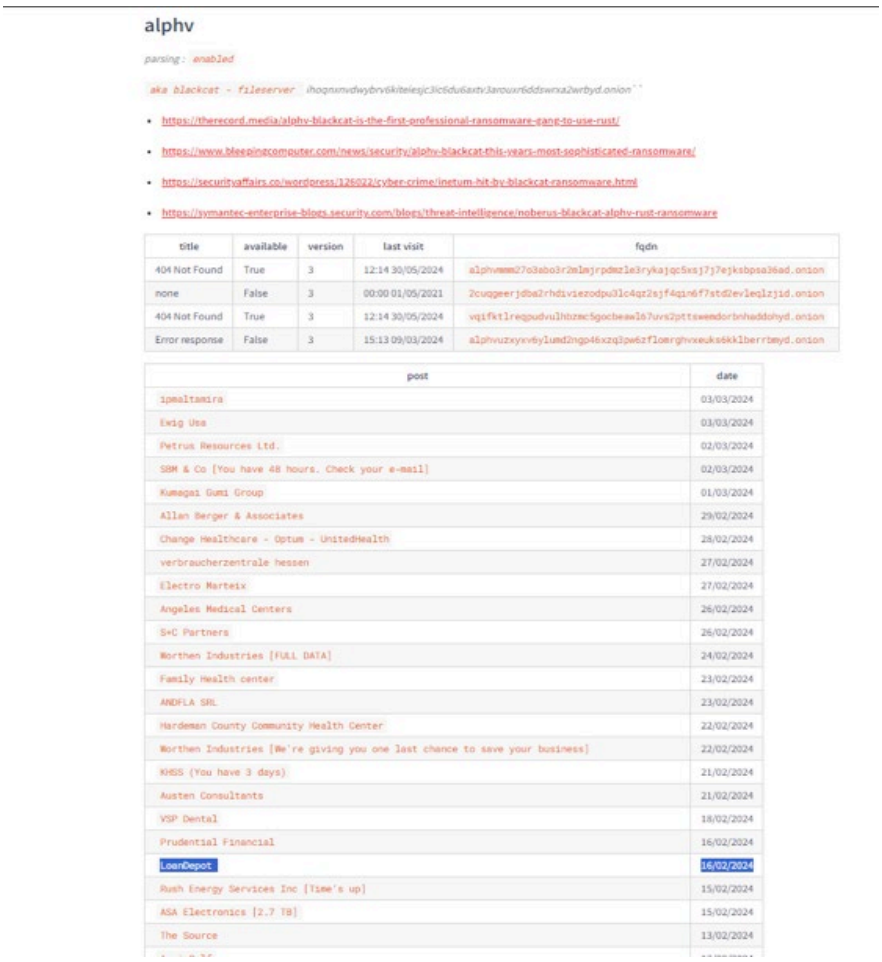
//

//

//

[24] *Id.*

[25] *Id.*



alphv

parsing : enabled

aka blackcat - fileserver ihoqnxnvdwybrv6kbtelesjc3ic6du6axtv3arouxr6ddswrxa2wr6yd.onion

- https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/
- https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/
- https://securityaffairs.co/wordpress/126022/cyber-crime/inetum-hit-by-blackcat-ransomware.html
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware

title	available	version	last visit	fqdn
404 Not Found	True	3	12:14 30/05/2024	alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion
none	False	3	00:00 01/05/2021	2cuqgeerjdba2rhd1viezodpu3lc4qz2sjf4qin6f7std2evleqlzjid.onion
404 Not Found	True	3	12:14 30/05/2024	vqifktlreqpudvulhbzmc5gocheawl67uvs2pttswemdorbnheddohyd.onion
Error response	False	3	15:13 09/03/2024	alphvuzxyxv6ylumd2ngp46xzq3pw6zflomrghvxeuks6kklberrbmyd.onion

post	date
ipmaltamira	03/03/2024
Ewig Usa	03/03/2024
Petrus Resources Ltd.	02/03/2024
SBM & Co [You have 48 hours. Check your e-mail]	02/03/2024
Kumagai Gumi Group	01/03/2024
Allan Berger & Associates	29/02/2024
Change Healthcare - Optum - UnitedHealth	28/02/2024
verbraucherzentrale hessen	27/02/2024
Electro Marteix	27/02/2024
Angeles Medical Centers	26/02/2024
S+C Partners	26/02/2024
Worthen Industries [FULL DATA]	24/02/2024
Family Health center	23/02/2024
ANDFLA SRL	23/02/2024
Hardeman County Community Health Center	22/02/2024
Worthen Industries [We're giving you one last chance to save your business]	22/02/2024
KHSS (You have 3 days)	21/02/2024
Austen Consultants	21/02/2024
VSP Dental	18/02/2024
Prudential Financial	16/02/2024
LoanDepot	16/02/2024
Rush Energy Services Inc [Time's up]	15/02/2024
ASA Electronics [2.7 TB]	15/02/2024
The Source	13/02/2024

109. Subsequently on or about February 23, 2024, almost six weeks after the January 8, 2024 announcement and SEC filing, Defendant finally began to provide notice of the Data Breach to its customers, employees, and states' attorneys general.[26] The size of this already massive breach grew to 16,924,071. Defendant also offered 24 months of single-bureau credit monitoring through Experian.

110. Defendant's disclosures did not mention anything about the threat actor, or the fact that highly confidential Private Information including SSNs was exfiltrated by a well-known ransomware gang that publicly announced it was in the final stages of selling the data. Instead, the Notice Letters speak in vague terms about customer data that "may have been accessed."[27]

[26] *See*, *supra*, n. 1.
[27] *Id.*

111. The unreasonable delay of action and prolonged exposure of almost 17 million customers' Private Information has unreasonably exacerbated the harms caused by the Data Breach by denying affected individuals the opportunity to proactively protect their Private Information from misuse as a result of the Data Breach.

112. Defendant acknowledged in a subsequent Form 8-K filing that the attackers not only acquired customer data, but that they also "access[ed] certain Company systems," encrypted data, and forced Defendant to shut down customer portals and other tools in response to the attack.[28]

113. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information. Defendant could also have employed multi-factor authentication to ensure that compromised passwords could not be used by unauthorized individuals.

114. A ransomware attack is a type of cyberattack that is frequently used to target companies due to the sensitive data they maintain.[29] In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[30]

115. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware

[28] Sergiu Gatlan, *US mortgage lender loanDepot confirms ransomware attack*, BleepingComputer (Jan. 8, 2024, 12:39 p.m.), https://www.bleepingcomputer.com/news/security/us-mortgage-lender-loandepot-confirms-ransomware-attack/.

[29] Danny Palmer, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, ZDNET (July 14, 2020, 8:28 a.m. PT), https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[30] *Ransomware FAQs*, Stop Ransomware, https://www.cisa.gov/stopransomware/ransomware-faqs (last visited May 30, 2024).

groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[31] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."[32]

116. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack, in which the attacker encrypts a network and exfiltrates the data contained within.[33] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[34] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[35] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[36]

117. Based upon the public statements of the threat actors, their reputation for "triple extortion" ransomware attacks, and Defendant's own Form 8-K statement acknowledging exfiltration, this ransomware attack was designed to not just encrypt Defendant's systems, but also to steal and monetize massive amounts of Private Information.

118. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for

---

[31] *Ransomware: The Data Exfiltration and Double Extortion Trends*, Center for Internet Security, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last visited May 30, 2024).

[32] *The chance of data being stolen in a ransomware attack is greater than one in ten*, Emsisoft Malware Lab (July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

[33] *Id.*

[34] *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, Coveware (November 4, 2020), https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

[35] *Id*.

[36] *Id*.

protection."[37]

119. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States government, the following measures:

- 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;
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;
- 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;
- Set anti-virus and anti-malware programs to conduct regular scans automatically;
- 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 written 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

[37] *How to Protect Your Networks from Ransomware*, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited May 30, 2024).

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; and
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[38]

120. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, several measures, including applying the latest security updates, thoroughly investigating and mediating alerts, collaborating with IT professionals about security operations, using multifactor authentication and network-level authentication, and strengthening Defendant's infrastructure.[39]

121. Given that Defendant was storing the sensitive Private Information of its current and former customers and applicants, Defendant could and should have implemented the above measures to prevent and detect cyberattacks.

122. In response to the Data Breach, loanDepot admits it worked with external "security experts" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. loanDepot admits additional security was

[38] *Id.* at 3-4.

[39] Microsoft Threat Intelligence, *Human-operated Ransomware Attacks: A Preventable Disaster,* Microsoft (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

required, but there is no indication whether these steps are adequate to protect Plaintiffs' and Class Members' Private Information going forward.

C. loanDepot Had Ample Notice of Its Computer Systems' Vulnerabilities and That It Was a Likely Cyberattack Target

123. Given the valuable Private Information that Plaintiffs and Class Members entrusted loanDepot with, its prior data breach and the escalating frequency of cyberattacks in the finance industry, loanDepot knew, or should have known, at all relevant times, that it was vulnerable to and at a heightened risk of cyberattacks.

124. loanDepot was on notice that it was actively targeted by hackers. In August 2022, loanDepot was subject to a separate cyberattack. The attack exposed tens of thousands of documents that included customers' Private Information and impacted well over a thousand individuals.[40]

125. Nine months after the August 2022 breach, on May 8, 2023, loanDepot notified customers that their information had been stolen in a cyberattack.[41] In light of the stringent laws mandating companies to immediately report data breaches, loanDepot's failure to report the August 2022 data breach for nine months suggests that loanDepot's systems were so deficient and inadequate that loanDepot did not know, for an unreasonably protracted period, that it had been hacked.

126. loanDepot knew or should have known the high probability of additional sophisticated attacks, and that additional significant security measures were necessary to prevent further breaches. Nonetheless, despite the significant August 2022 data breach, loanDepot failed to invest adequate resources required to improve its data security, thus continuing to expose its customers to a foreseeable and significant risk of another data breach.

---

[40] *Data Security Event*, loanDepot (April 24, 2023), https://www.doj.nh.gov/consumer/security-breaches/documents/loandepot-20230424.pdf.

[41] *Id.*

127. In addition to being on notice of its systems' security vulnerabilities following its August 2022 data breach, loanDepot knew or should have known that it was at a heightened risk of a cyberattack due to the surge of cyberattacks and/or data breaches the mortgage industry was and has been experiencing.

128. In October 2023, in response to the increasing prevalence of cyberattacks in the mortgage and real estate industry, the United States Federal Trade Commission ("FTC") finalized an amendment to the Safeguards Rule that requires mortgage originators, like loanDepot, to report certain data breaches and other security events affecting 500 or more customers to the FTC as soon as possible, but no later than 30 days.

129. In the third quarter of the 2023 fiscal year alone, 733 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[42]

130. Due to high profile data breaches at other large companies and because these attacks have become ubiquitous, Defendant knew or should have known that it was a prime target due to the vast amount of Private Information that it collected and maintained in the regular course of its business.

131. The increase in such attacks, and attendant risk of future cyberattacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

132. Defendant's CEO Frank Martel publicly affirmed loanDepot's knowledge of these risks when he stated: "we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared."[43]

[42] *ITRC Q3 Data Breach Analysis*, Identity Theft Resource Center, https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last visited May 30, 2024).

[43] *See*, *supra*, n. 4.

133. Given loanDepot's firsthand knowledge of its vulnerabilities to cyberattacks derived from its prior separate data breach in 2022, coupled with the prevailing industry knowledge of the pervasive uptick of data breaches, loanDepot knew or should have known that it was at a heightened risk of another data breach.

134. In light of the known risks and in violation of its representations to Class Members and its legal obligations, loanDepot failed to act to implement reasonable, expected, and readily available data security procedures and practices to protect against disclosure of its customers' Private Information.

D. loanDepot Failed to Comply with FTC Guidelines and Requirements

135. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

136. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[44] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[45] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[46]

---

[44] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (October 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[45] *Id.*

[46] *Id.*

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

138. Pursuant to Section 5 of the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. § 45, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data. The FTC has treated the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair business practice.

139. Orders resulting from these actions, including actions against mortgage lenders, further clarify the measures businesses must take to meet their data security obligations.

140. Defendant owed a duty to safeguard Plaintiffs' and Class Members' Private Information under FTC Act, 15 U.S.C. § 45, among other statutes further discussed below, to ensure that all information it received, maintained, and stored was secure. These statutes were enacted to protect Plaintiffs and Class Members from the type of conduct in which Defendant engaged and the resulting harms Defendant caused Plaintiffs and Class Members.

141. Defendant failed to properly implement basic data security measures to protect against unauthorized access to customer Private Information, which constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

142. Had Defendant exercised reasonable care and properly maintained and adequately protected its systems, servers, and networks in accordance with its duties, the Data Breach would not have occurred or would have been detected and prevented.

E. loanDepot Failed to Comply with Industry Standards

143. As noted above, experts studying cyber security routinely identify

mortgage lenders and partners as being particularly vulnerable to cyberattacks because of the volume of the valuable Private Information which they collect and maintain.

144. Several best practices that, at a minimum, should be implemented by companies that maintain Private Information, like Defendant, include but are not limited to: educating and training all employees; strong passwords; changing passwords frequently; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; retaining Private Information for limited amounts of time, and limiting access to sensitive data.

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

146. Defendant also failed to meet the minimum standards 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.

147. The foregoing frameworks are applicable industry standards in the mortgage industry. Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

148. Defendant's failure to comply with industry standard data security practices was directly contrary to the representations made to its customers and consumers in its Privacy Policy and constitutes material misrepresentations.

F. loanDepot Breached Its Duties to Plaintiffs and Class Members

149. As a sophisticated business entity handling confidential Private Information, loanDepot's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of Private Information preceding the date of the Data Breach.

150. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect them from unauthorized access and disclosure.

151. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow, and intentionally misrepresented to Plaintiffs and Class Members the actions that it would take to protect their confidential information. Defendant's breaches of obligations include, but are not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. failing to adequately protect Private Information;

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

d. failing to ensure that its vendors with access to their computer systems and data employed reasonable security procedures;

e. failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

f. failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software

programs that have been granted access rights;

g. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;

j. failing to train all members of its workforces effectively on the policies and procedures regarding Private Information;

k. failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

m. failing to adhere to industry standards for cybersecurity as discussed above; and

n. otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

152. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing third parties to access Defendant's unsecured and internet accessible networks, and to acquire and exfiltrate the unencrypted Private Information.

153. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized measures to mitigate damages, protect against adverse consequences, and thwart future misuse of Private Information. loanDepot further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In doing so, Defendant actually and proximately

caused and exacerbated Plaintiffs and Class Members' harm from the Data Breach and the injuries-in-fact.

154. Accordingly, as outlined below and in addition to other injuries resulting from the Data Breach, Plaintiffs and Class Members now face a continuing and imminent risk of fraud and identity theft. Moreover, due to the immutable information (e.g., SSNs) compromised in the Data Breach, Plaintiffs and Class Members will remain under this threat for the remainder of their lives.

G. Plaintiffs' and Class Members' Private Information is Highly Valuable

155. Private Information is an extremely valuable property right.[47] The value of sensitive personal information as a commodity is measurable.[48] Firms are now able to attain significant market valuations by employing business modes predicated on successful use of personal data within the existing legal and regulatory frameworks.[49]

156. Private Information is particularly valuable because criminals can use it to target victims with frauds and scams on an ongoing basis, rather than exploiting one account until it is canceled.

157. Private Information demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security

---

[47] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[48] Robert Lowes, *Stolen EHR Charts Sell for $50 Each on Black Market*, Medscape (April 28, 2014), https://www.medscape.com/viewarticle/824192?form=fpf.

[49] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLibrary (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

Numbers are worth more than 10x on the black market."[50]

158. According to the United States Government Accountability Office ("USGAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[51]

159. Private Information is such a valuable commodity to identity-thieves that once the information has been compromised, it is circulated and traded by criminals on the "cyber black-market" for years.

160. Because of the value of its collected and stored data, the financial industry has experienced disproportionally higher numbers of data theft events than other industries.

161. Based upon the public statements of the threat actors that they were in the final stages of selling the stolen data, there is a likelihood that entire batches of stolen information have already been dumped on the black market, or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for the foreseeable future and beyond.

162. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[52]

163. The data marketplace is so sophisticated that consumers can actually sell

---

[50] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[51] *See, supra*, n. 13.

[52] Ashiq JA, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

their non-public information directly to a data broker who, in turn, aggregates the information and provides it to marketers or app developers.[53,54]

164. For instance, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[55]

165. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

166. Defendant knew, or should have known, about these dangers and should have strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

H. The Data Breach Has and Will Continue to Cause Disruption and Increased Risk of Fraud and Identity Theft

167. Cyberattacks and data breaches at mortgage companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

168. The USGAO released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[56]

---

[53] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, Los Angeles Times (Nov. 5, 2019, 5:00 a.m. PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[54] Datacoup, Inc. Home Page, https://datacoup.com/ (last visited May 30, 2024).

[55] *See* https://digi.me/what-is-digime/ (last visited May 30, 2024).

[56] *Supra*, n. 13.

169. That is because a data breach victim is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal Private Information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or SSN. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages, or phishing emails.

170. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (or an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[57]

171. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

172. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's picture, use the victim's name and SSN to obtain government benefits, or file a fraudulent tax return using the

[57] *IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 1, 2024).

victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. Each of these fraudulent activities is difficult to detect. An individual may not know that their SSN was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

173. Moreover, it is not an easy task to change, or cancel, a stolen SSN:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[58]

174. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

175. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[59]

---

[58] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015, 4:59 a.m. ET), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

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

176. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

177. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

178. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

179. Thus, the information stolen in the Data Breach makes it easy for criminals to create a comprehensive "Fullz" package of Plaintiffs and Class Members, which can be sold and resold in perpetuity.

V. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

180. Numerous Plaintiffs have already suffered from actual misuse of the data

---

ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014, 10:40 a.m.), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

compromised in this Data Breach, and have suffered other concrete injuries (including lost time) as a result of that actual misuse.

181. As a direct and proximate cause of Defendant's Data Breach, Plaintiffs and Class Members face imminent, perpetual, and irreparable harm to their personal, financial, reputational, and future well-being.

182. Notably, there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it also sometimes takes years for others to learn that information.[60]

183. For example, the Social Security Administration has warned that identity thieves can use an individual's SSN to apply for additional credit lines.[61] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen SSNs also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[62] Each of these fraudulent activities is difficult to detect. An individual may not know that her or her SSN was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

184. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close"

[60] John W. Coffey, Difficulties in Determining Data Breach Impacts, SYSTEMICS, CYBERNETICS AND INFORMATICS (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf (last visited May 1, 2024).
[61] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 30, 2024).
[62] *Id* at 4.

and difficult, if not impossible, to change, e.g., SSNs, addresses, and names.

185. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[63]

186. To date, Defendant has done little to provide Plaintiffs and the Class Members with relief for the damages they have suffered because of the Data Breach.

187. As a direct and proximate result of Defendant's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiffs' and Class members' Private Information, and Defendant's failure to properly and timely notify Plaintiffs and Class members, Plaintiffs and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, medical fraud, and/or other unauthorized uses of personal information;
b. money and time lost as a result of fraudulent access to and use of their accounts, including financial accounts;
c. loss of use of and access to their financial accounts and/or credit;
d. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
f. lowered credit scores resulting from credit inquiries following fraudulent activities;

[63] *See, supra*, n. 50.

g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

h. costs and lost time obtaining credit reports in order to monitor their credit records;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their Private Information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendant fails to undertake appropriate, legally required steps to protect the personal information in its possession.

188. As a result of the events detailed herein, many victims have already suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. This includes without limitation:

- reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- purchasing credit monitoring and identity theft prevention;
- placing "freezes" and "alerts" with reporting agencies;
- spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- contacting financial institutions and closing or modifying financial accounts; and
- closely reviewing and monitoring SSNs, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

189. Plaintiffs and Class Members have suffered and will continue to suffer from various forms of harm and privacy violations due the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Private Information.

190. Plaintiffs and Class Members were also damaged in that they overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's systems and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to, and were deprived of the benefit of their bargain.

191. Further, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the fear, anxiety, and stress that

their Private Information may be disclosed at any moment to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy. This emotional distress goes beyond allegations of mere worry or inconvenience—it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

VI. CLASS ACTION ALLEGATIONS

192. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Nationwide Class and State Subclass definitions (collectively the "Class"), subject to amendment as appropriate:

Nationwide Class

All persons in the United States whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent notice (the "Nationwide Class").

Arizona Subclass

All persons in the state of Arizona whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "Arizona Subclass").

California Subclass

All persons in the state of California whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "California Subclass").

Colorado Subclass

All persons in the state of Colorado whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "Colorado Subclass").

Florida Subclass

All persons in the state of Florida whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "Florida Subclass").

Illinois Subclass

All persons in the state of Illinois whose data was impacted or otherwise

compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "Illinois Subclass").

Maine Subclass

All persons in the state of Maine whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "Maine Subclass").

New York Subclass

All persons in the state of New York whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "New York Subclass").

North Carolina Subclass

All persons in the state of North Carolina whose data was impacted or otherwise compromised by the Data Breach reported by loanDepot in January 2024, including all those who were sent Notice (the "North Carolina Subclass").

193. All members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach.

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

195. Plaintiffs reserve the right to amend or propose additional classes or subclasses upon conducting discovery.

196. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

197. **Numerosity.** The Members of the Class are so numerous that joinder of all of them is impracticable. The approximate number of Nationwide Class Members is 16.9 million. The exact number of members belonging to each Subclass is unknown to Plaintiffs at this time, based on information and belief and loanDepot's public

disclosures, the Subclasses consists of millions of individuals whose sensitive data was compromised in the Data Breach.

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

- if Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.
- if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- if Defendant owed a duty to Class Members to safeguard their Private Information;
- if Defendant breached their duty to Class Members to safeguard their Private Information;
- if Defendant knew or should have known that their data security systems and monitoring processes were deficient;
- if Defendant should have discovered the Data Breach sooner;
- if Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- if Defendant's conduct was negligent;
- if Defendant's breach implied contracts with Plaintiffs and Class Members;
- if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

//

- if Defendant failed to provide notice of the Data Breach in a timely manner; and
- if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

199. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

200. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

201. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

protects the rights of each Class Member.

203. **Declaratory and Injunctive Relief.** In addition, Defendant has acted and/or refused to act on grounds that apply generally to the Nationwide Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the personally identifiable information of Nationwide Class Members, (2) fail to adequately protect Class Members' personally identifiable information, and (3) violate Class Members' rights under numerous state consumer protection laws and other claims alleged herein. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

204. Particular issues under Rule 42(d)(l) are also appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues were set forth above, and include, but are not limited to, whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach, and whether Defendant's security measures were reasonable.

VII. CHOICE OF LAW

205. The loanDepot website Terms of Use state, "This Agreement and the resolution of any dispute related to this Agreement or this Site shall be governed by and construed in accordance with the laws of California without giving effect to any principles of conflicts of law," indicating loanDepot's intent to be governed by the laws of California in the procuring and management of loans.[64]

206. loanDepot elected to have California law govern all claims and disputes concerning the website at issue in this lawsuit. Accordingly, the application of

[64] *Terms of Use*, loanDepot, https://www.loandepot.com/termsofuse (last visted June 3, 2024).

California law to all of the Class Members' claims is fair, appropriate, and an election affirmatively made by loanDepot consistent in its agreements.

207. Beyond loanDepot's election of California law to govern the claims described herein, the State of California has a significant interest in regulating the conduct of businesses operating within its borders. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company headquartered and doing business in California, has a greater interest in the claims of Plaintiffs and class members than any other state or country and is most intimately concerned with the claims and outcome of this litigation.

208. The principal place of business of loanDepot, located at 6561 Irvine Center Drive, Irvine, California, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its marketing, software development, and major policy, financial, and legal decisions.

209. loanDepot's response to the allegations herein, and corporate decisions surrounding such response, were made from and in California.

210. loanDepot's breaches of duty to Plaintiffs and the Class emanated from California, and the website at issue herein, on information and belief, was designed, created, and tested in California.

211. Application of California law with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because California has a state interest in the claims of the Plaintiffs and the Class based upon loanDepot's significant and ongoing contacts with California.

212. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the common law claims of all class members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's consumer protection laws may be applied to non-resident Plaintiffs and class members.

VIII. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

213. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

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

215. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

216. Defendant has a duty to Plaintiffs and Class Members to safeguard and protect their Private Information.

217. Defendant has a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with Private Information data.

218. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system – and Class Members' Private Information held within it – to prevent disclosure of the information, and to safeguard the information. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

219. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and all other requirements

discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

220. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and individuals who entrusted them with Private Information, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

221. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

222. Defendant breached its duty of care by failing to secure and safeguard the Private Information of Plaintiffs and Class Members. Defendant negligently stored and/or maintained its data security systems and published that information on the Internet.

223. Further, Defendant by and through its above negligent actions and/or inactions, breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, manage, monitor, and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' Private Information within its possession, custody and control.

224. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs' and Class Members' Private Information.

225. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, et seq.) ("GLBA"), the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, et seq. ("CCPA"), Cal. Civ. Code §§ 1798.80, et seq., the

Consumers Legal Remedies Act, the Customer Record's Act, among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale of lending products and services in order to safeguard Plaintiffs' and Class Members' Private Information.

226. Plaintiffs and the other Class Members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised Private Information subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either the use of the compromised information or access to their user accounts.

227. It was reasonably foreseeable – in that Defendant knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such Private Information, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

228. But for Defendant's negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

229. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

230. Plaintiffs and Class Members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION
Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant or, alternatively, the State Subclasses)

231. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

232. Plaintiffs and Class Members entered into a valid and enforceable contract through which they were required to turn over their sensitive personal information to Defendant in exchange for Defendant's services.

233. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' sensitive personal information to any third parties without their consent.

234. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its customers. Defendant's Privacy Policy and/or the representations contained therein were provided to Plaintiffs and Class Members in a way that it became part of the agreement for services with Defendant.

235. Aside from state and federal laws, regulations, and industry standards, through the Privacy Policy, Defendant committed to protecting the privacy and security of the sensitive Private Information and promised to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

236. Plaintiffs and Class Members performed substantially all that was required of them under their contract with Defendant, or they were excused from doing so.

237. Defendant failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs and Class Member's Private Information.

238. Defendant also violated the covenant of good faith and fair dealing by its conduct alleged herein.

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

240. Plaintiffs and Class Members have complied with and performed all, or substantially all, of the obligations imposed on their conditions with Defendant.

241. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard its customers' Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

242. Defendant breached the implied covenant of good faith and fair dealing by, among other things:

- disclosing Plaintiffs' and other Class Members' personal information to unauthorized third parties;
- allowing third parties to access the personal information of Plaintiffs and other Class Members;
- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs and other Class Members of the unlawful disclosure of their personal information; and
- failing to maintain adequate security and proper encryption in Defendant's websites, customer portals, and services.

243. As a direct and proximate result of Defendant's breach of contract, or its independent breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members did not receive the benefit of the bargain, and instead, the services they acquired from Defendant were less valuable than described in their contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at

least equal to the difference in value between that which was promised and Defendant's deficient performance.

244. Also, as a result of Defendant's breach of contract, or its independent breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from the exposure of their Private Information, and they remain at imminent risk of suffering additional damages in the future.

245. Accordingly, Plaintiffs and Class Members have been injured by Defendant's breach of contract and are entitled to damages, including nominal damages, and/or restitution in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant or, alternatively, the State Subclasses)

246. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

247. Defendant provides mortgages, loans, or other financial services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through its collective conduct, including by Plaintiffs and Class Members providing their Private Information to Defendant in exchange for the services offered.

248. Through Defendant's offering of these lending and financial services, it knew or should have known that it needed to protect Plaintiffs' and Class Members' confidential Private Information in accordance with their own policies, practices, and applicable state and federal law.

249. As consideration, Plaintiffs and Class Members turned over valuable Private Information relying on Defendant to securely maintain and store their Private Information in return and in connection with their services.

//

250. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing its services, including data security, to Plaintiffs and Class Members.

251. In delivering their Private Information to Defendant in exchange for their services, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard their Private Information as part of those services.

252. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to Private Information to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designating and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; and (6) taking other steps to protect against foreseeable data breaches.

253. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

254. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, including but not limited to Defendant's decision to continue to collect, store, and maintain Plaintiffs' and Class Members' Private Information despite knowledge of Defendant's previous data breach, Plaintiffs and Class Members would not have agreed to provide their Private Information to Defendant.

255. As providers of mortgage, lending, and financial services, Defendant recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of

material importance as part of the bargain with Plaintiffs and the Class.

256. A meeting of the minds occurred, and an implied contract was formed, as Plaintiffs and Class Members agreed, *inter alia*, to provide their accurate and complete sensitive personal information to Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Private Information.

257. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures and supervision of its systems and networks, as well as its vendors, business associates, and/or suppliers, to secure Plaintiffs' and Class Members' Private Information.

258. Defendant also violated the covenant of good faith and fair dealing by its conduct alleged herein.

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

260. Plaintiffs and Class Members have complied with and performed all, or substantially all, of the obligations imposed on their conditions with Defendant.

261. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard its customers' Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

262. Defendant breached the implied covenant of good faith and fair dealing by, among other things:

- disclosing Plaintiffs' and other Class Members' personal information to unauthorized third parties;
- allowing third parties to access the personal information of

Plaintiffs and other Class Members;

- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs and other Class Members of the unlawful disclosure of their personal information; and
- failing to maintain adequate security and proper encryption in Defendant's websites, customer portals, and services.

263. Plaintiffs and Class Members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

264. Accordingly, Plaintiffs and Class Members have been injured by Defendant's breach of contract and are entitled to damages, including nominal damages, and/or restitution in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or, alternatively, Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass)

265. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

266. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass.

267. Plaintiffs and Class Members had a legally protected privacy interest and a reasonable expectation of privacy in the Private Information that Defendant required them to provide, stored, and mishandled.

268. California established the right to privacy in Article 1, Section 1 of the California Constitution.

269. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of

Torts which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977).

270. Plaintiffs and Class Members reasonably expected that their Private Information would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

271. Defendant owed a duty to customers in its network, including Plaintiffs and Class members, to keep their Private Information confidential.

272. The unauthorized release of Private Information is highly offensive to a reasonable person.

273. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class Members by (a) failing to adequately secure their Private Information from disclosure to unauthorized parties for improper purposes; (b) disclosing their Private Information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their Private Information to unauthorized parties without the informed and clear consent of Plaintiffs and Class Members. This invasion into the privacy interest of Plaintiffs and Class Members is serious and substantial.

274. In failing to adequately secure Plaintiffs' and Class Members' Private Information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its substandard security measures would cause its users harm and, would be considered highly offensive to a reasonable person in the same position as Plaintiffs and Class Members.

275. Defendant violated Plaintiffs' and Class Members' right to privacy under California law, including, but not limited to California common law and Article 1, Section 1 of the California Constitution and the California Consumer Privacy Act.

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

277. 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, Defendant intentionally invaded Plaintiffs and Class Members' privacy by:

- 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;
- Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and
- Intentionally causing anguish or suffering to Plaintiffs and Class Members.

278. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiffs and Class members.

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

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

281. Defendant concealed from and delayed reporting to Plaintiffs and Class Members the Data Breach that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

282. The conduct described above was directed at Plaintiffs and Class Members.

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

284. In failing to protect Plaintiffs' and Class Members' Private Information, and in misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf themselves and the Class.

285. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

286. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs' and Class Members' Private Information has been accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and proposed Class Members have suffered injuries as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

287. Plaintiffs and Class Members are entitled to injunctive relief as well as actual and punitive damages.

FIFTH CAUSE OF ACTION
Violations of the California Consumer Privacy Act
California Civil Code § 1798.150
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or, alternatively, Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass)

288. Plaintiffs re-allege and incorporate by reference all other paragraphs of

this complaint as though fully set forth herein.

289. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass.

290. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . 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 damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

291. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs' and the Class's nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

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

293. Plaintiffs and California Subclass Members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

294. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiffs' and Class Members' Private Information.

295. Plaintiffs and Class Members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

296. Defendant has long had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous related actions against it arising from the Data Breach, the first of which were filed on or about January 19, 2024. Further, Defendant is the party with the most knowledge of the underlying facts giving rise to Plaintiffs' allegations, so that any pre-suit notice would not put Defendant in a better position to evaluate those claims. Plaintiffs further sent Defendant notice consistent with the CCPA on or before May 3, 2024. Based on information and belief, additional plaintiffs in related actions further provided Defendant with CCPA notice beginning on or about February 5, 2024.

297. Defendant failed to take sufficient and reasonable measures to safeguard its data security systems and protect Plaintiffs' and California Subclass Members' highly sensitive personal information and medical data from unauthorized access. Defendant's failure to maintain adequate data protections subjected Plaintiffs' and the California Subclass Members' nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

298. The unauthorized access, exfiltration, theft, and disclosure of Plaintiffs and the California Subclass Members' Private Information was a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

299. Under Defendant's duty to protect customers' Private Information, it was required to implement reasonable security measures to prevent and deter hackers from accessing the Private Information of its customers. These vulnerabilities existed and enabled unauthorized third parties to access and harvest customers' Private Information, evidence that Defendant has breached that duty.

300. Plaintiffs and California Subclass Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

301. Defendant's violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

302. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PHI/Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

303. Plaintiffs are further entitled to the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

SIXTH CAUSE OF ACTION
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL")
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass)

304. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

305. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass.

306. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

307. By reason of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and Class members' Private Information, Defendant engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

308. The acts, omissions, and conduct complained of herein in violation of the UCL were designed and emanated from Defendant's California corporate office.

309. Plaintiffs suffered injury, in fact, and lost money or property as a result of Defendant's alleged violations of the UCL.

310. The acts, omissions, and conduct of Defendant as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

311. Defendant violated the unlawful prong of the UCL by violating, inter alia, the CCPA, CCRA, GLBA, and FTC Act as alleged herein.

312. Defendant violated the unlawful prong of the UCL by failing to honor the terms of its implied contracts with Plaintiffs and Class Members, as alleged herein.

313. Defendant's conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, et seq., the CCPA concerning consumer privacy, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

//

//

Unfair Prong

314. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because Defendant's acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and other Class Members. The gravity of Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

315. Defendant's failure to utilize, and to disclose that it does not utilize, industry standard security practices, constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendant's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendant has not—to the detriment of its customers and to competition.

Fraudulent Prong

316. By failing to disclose that it does not enlist industry-standard security practices, all of which rendered Class Members particularly vulnerable to data breaches, Defendant engaged in UCL-violative practices.

317. A reasonable consumer would not have transacted with Defendant if they knew the truth about its security procedures. By withholding material information about its security practices, Defendant was able to obtain customers who provided and entrusted their Personal Information in connection with transacting business with Defendant. Had Plaintiffs known the truth about Defendant's security procedures, Plaintiffs would not have done business with Defendant.

318. As a result of Defendant's violations of the UCL, Plaintiffs and Class Members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard data security measures for the

collection, storage, and retention of customer data; (2) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (3) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendant purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendant, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information.

319. As a result of Defendant's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact with Defendant or made purchases or spent money that they otherwise would not have made or spent, had they known the true state of affairs regarding Defendant's data security policies. Class Members lost control over their

Private Information and suffered a corresponding diminution in value of that Private Information, which is a property right. Class Members lost money as a result of dealing with the fallout of and attempting to mitigate harm arising from the Data Breach.

320. Plaintiffs request that the Court issue sufficient equitable relief to restore Class Members to the position they would have been in had Defendant not engaged in violations of the UCL, including by ordering restitution of all funds that Defendant may have acquired from Plaintiffs and Class Members as a result of those violations.

SEVENTH CAUSE OF ACTION
Violations of the California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq*. ("CCRA")
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass)

321. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

322. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass.

323. Under the California Consumer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Id. (emphasis added).

//

324. The Data Breach constitutes a "breach of the security system" of Defendant. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and Class Members.

325. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class but waited to notify them. Given the severity of the Data Breach, this is an unreasonable delay.

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

327. As a direct or proximate result of Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

328. Plaintiffs accordingly requests that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendant utilize strong industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendant, consistent with industry standard practices, engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (3) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendant purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its

provisions of services; (7) ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendant, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information.

329. Plaintiffs and Class Members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

EIGHTH CAUSE OF ACTION
Violations of the California Consumer Legal Remedies Act
Remedies Act, California Civil Code § 1750, *et seq*.
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass)

330. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

331. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class and the Nationwide Class, or, alternatively, California Plaintiffs Krieghauser, Isaiah, and Singh and the California Subclass.

332. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq*.

333. Defendant has long had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous related actions against it arising from the Data Breach, the first of which were filed on or about January 19, 2024. Further, Defendant is the party with the most knowledge of the underlying facts giving rise to

Plaintiffs' allegations, so that any pre-suit notice would not put Defendant in a better position to evaluate those claims. Plaintiffs further sent Defendant notice consistent with the CLRA on or before May 3, 2024. Based on information and belief, additional plaintiffs in related actions further provided Defendant with CLRA notice beginning on or about February 5, 2024.

334. To the extent the Court finds Plaintiffs have still not met the CLRA notice requirements, Plaintiffs in the alternative seek only injunctive relief pursuant to Cal. Civ. Code § 1782, subdivision (d), which provides that "[a]n action for injunctive relief brought under the specific provisions of Section 1770 may be commenced without compliance with subdivision (a)."

335. Plaintiffs and Nationwide Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

336. Plaintiffs, Nationwide Class Members, and Defendant have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

337. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendant was likely to deceive consumers.

338. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

339. Defendant violated this provision by representing that it took appropriate measures to protect Plaintiffs' and the Nationwide Class Members' Private Information.

340. Additionally, Defendant improperly handled, stored, or protected either unencrypted or partially encrypted data.

341. As a result, Plaintiffs and Nationwide Class Members were induced to enter into a relationship with Defendant and provide their Private Information.

//

342. Defendant intended to, and did, mislead Plaintiffs and Class Members and induced them to rely on its misrepresentations and omissions.

343. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class Members' Private Information as part of the services Defendant provided and for which Plaintiffs and Class Members paid without advising Plaintiffs and Class Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Private Information. Accordingly, Plaintiffs and the Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

344. As a result of engaging in such conduct, Defendant has violated Civil Code § 1770.

345. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiffs seek an order of this Court that includes, but is not limited to, an order enjoining Defendant from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

346. Plaintiffs and Class Members suffered injuries caused by Defendant's misrepresentations, because they provided their Private Information believing that Defendant would adequately protect this information.

347. Plaintiffs and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

348. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiffs and Class Members.

349. Plaintiffs seek prospective injunctive relief, including improvements to Defendant's data security systems and practices, in order to ensure that such security

is reasonably sufficient to safeguard customers' Private Information that remains in Defendant's custody, including but not limited to the following:

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

B. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

C. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

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

E. Ordering that Defendant not transmit Private Information via unencrypted email;

F. Ordering that Defendant not store Private Information in email accounts;

G. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for provisions of Defendant's services;

H. Ordering that Defendant conduct regular computer system scanning and security checks;

I. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in

response to a breach; and

J. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

350. Unless such Class-wide injunctive relief is issued, Plaintiffs and Class Members remain at risk, and there is no other adequate remedy at law that would ensure that Plaintiffs (and other consumers) can rely on Defendant's representations regarding its data security in the future.

351. Furthermore, in the alternative to all legal remedies sought herein, Plaintiffs, on behalf of the Class, seek monetary relief including but not limited to all damages recoverable under the CLRA, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices; restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices; declaratory relief; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

NINTH CAUSE OF ACTION
Violations of the Florida Deceptive and Unfair Trade Practices Act Fla. Stat. § 501.201, *et. seq.*
(On Behalf of Plaintiff Jessica Schuler and the Florida Subclass Against Defendant)

352. Plaintiff Jessica Schuler ("Plaintiff" for the purposes of this count) re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein and brings this claim on behalf of herself and the Florida Subclass (the "Class" for the purposes of this count).

353. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained Plaintiff's and the Class Members' Private Information through advertising,

soliciting, providing, offering, and/or distributing goods and services to Plaintiff and the Class Members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

354. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

- failure to implement adequate data security practices to safeguard Plaintiff's and Class Members' Private Information;
- failure to make only authorized disclosures of customers' and applicants' Private Information;
- failure to disclose that their data security practices were inadequate to safeguard customers' Private Information from theft; and
- failure to timely and accurately disclose the Data Breach to Plaintiff and Class Members.

355. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's current and former customers and/or applicants.

356. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices by omitting, failing to disclose, or inadequately disclosing to Defendant's current and former customers and applicants that it did not follow industry best practices for the collection, use, and storage of Private Information.

357. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class Members are entitled to recover an order providing declaratory relief and reasonable attorneys' fees and costs, to the extent permitted by law.

358. Also, as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class Members are entitled to injunctive relief, including, but not limited to:

- ordering that Defendant implement measures that ensure that the Private Information of Defendant's current and former customers and applicants is appropriately encrypted and safeguarded when stored on Defendant's network or systems;
- ordering that Defendant purge, delete, and destroy in a reasonable secure manner Private Information not necessary for its provision of services;
- ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- ordering Defendant to meaningfully educate its current and former customers and applicants about the threats they face as a result of the accessibility of their Private Information to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

TENTH CAUSE OF ACTION
Violations of the New York Deceptive Trade Practices Act New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs Hernandez and Ricco-Brown and the New York Subclass Against Defendant)

359. Plaintiffs Hernandez and Ricco-Brown ("Plaintiffs" for the purposes of this count) re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein and brings this claim on behalf of himself and the New York Subclass (the "Class" for the purposes of this count).

360. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- misrepresenting material facts to Plaintiff and the Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members'

Private Information from unauthorized disclosure, release, data breaches, and theft;

- misrepresenting material facts to Plaintiffs and the Class by representing that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;
- omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Private Information;
- engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and
- engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

361. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiffs' and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

362. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

363. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendant's network and aggregation of Private Information.

364. The representations upon which consumers (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

//

365. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

366. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

367. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing employment benefit services to consumers in the State of New York.

368. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

369. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant

promised when Plaintiffs and the proposed Class entrusted Defendant with their Private Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Private Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiffs' and Class Members' Private Information.

370. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

ELEVENTH CAUSE OF ACTION
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 Ill. Comp. Stat. § 505/1, *et seq*.
(On Behalf of Plaintiff Debra Coe and Matthew McFall and the Illinois Subclass Against Defendant)

371. Plaintiff Debra Coe and Matthew McFall ("Plaintiffs" for the purposes of this count) re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein and bring this claim on behalf of themselves and the Illinois Subclass (the "Class" for the purposes of this count).

372. Plaintiffs and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

373. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

374. Plaintiffs may bring claims under the ICFA because there is a consumer nexus" between Plaintiff and consumers with respect to Defendant's unfair and deceptive trade practices.

375. Plaintiffs' actions were akin to a consumer's action because she justifiably relied on Defendant's public statements and omissions regarding its data security practices. Specifically, Defendant's statements, including its privacy policy, states Defendant will use reasonable security measures to protect its network from cybercriminals and ransomware attacks.

376. Defendant's representations and omissions as to its data security measures, and its failure to implement and maintain reasonable data security measures, concern all individuals because a reasonable consumer, akin to Plaintiffs, does or is reasonably likely to rely on these statements in providing their Private Information.

377. Defendant's conduct involved consumer protection concerns because Defendant represented to consumers and employees (current and former) that it employed proper data security measures but, in fact, did not. Defendant's conduct also involves consumer protection concerns because Defendant's failure to implement and maintain reasonable data security measures enabled third parties to access and exfiltrate the Private Information of consumers from its network. In turn, Plaintiffs' and Class Members' Private Information is now on the dark web.

378. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiffs' and the Class Members' sensitive Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiffs and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiffs and the Class; (iii) failing to disclose or omitting materials facts to Plaintiffs and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Private Information of Plaintiffs and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Class's Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

379. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs and the Class and defeat their reasonable expectations about the security of their Private Information.

380. Defendant intended that Plaintiffs and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

381. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiffs and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

382. As a result of Defendant's wrongful conduct, Plaintiffs and the Class were injured in that they never would have provided their Private Information to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

383. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and the Class have suffered harm as set forth in detail above.

384. The requested relief by Plaintiffs will assist consumers because it will require Defendant to enhance its data security practices. Specifically, the Complaint seeks injunctive relief, etc. Moreover, any monetary compensation will deter Defendant from additional and future data breach incidents.

TWELFTH CAUSE OF ACTION
Violation of the Arizona Consumer Fraud Act,
Ariz. Rev. Stat. § 44-1521, *et seq*.
(On Behalf of Plaintiff Ware and the Arizona Subclass)

385. Plaintiffs re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein and bring this claim on behalf of

themselves and the Nationwide Class, or, alternatively, Plaintiff Ware and the Arizona Subclass.

386. The ACFA provides that "[t]he act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

387. Defendant is a person as defined by Ariz. Rev. Stat. § 44-1521(6).

388. Defendant advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

389. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521(5)) in violation of Ariz. Rev. Stat. § 44-1522(A), including, but not limited to, the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous 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 Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it 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 FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not 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 FTC Act, 15 U.S.C. § 45.

390. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

391. Defendant intended to, and did, mislead Plaintiffs and Class Members and induced them to rely on its misrepresentations and omissions.

392. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable

data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class Members' Private Information as part of the services Defendant provided and for which Plaintiffs and Class Members paid without advising Plaintiffs and Class Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Private Information. Accordingly, Plaintiffs and the Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

393. Defendant acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Class Members' rights. Defendant were on notice that their security and privacy protections were inadequate and that they were targets of such attacks.

394. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, 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 and cancelling and replacing passports; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

395. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

THIRTEENTH CAUSE OF ACTION
Violation of the Colorado Consumer Protection Act
Colo. Rev. Stat. § 6-1-101, *et seq.*
(On Behalf of Plaintiff Beller and the Colorado Subclass)

396. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein and bring this claim on behalf of themselves and the Nationwide Class, or, alternatively, Plaintiff Beller and the

Colorado Subclass.

397. Defendant engaged in unlawful, unfair, and deceptive acts and practices, with respect to the sale and advertisement of services paid for by Plaintiffs and the Class Members in violation of Colo. Rev. Stat. § 6-1-105, including by representing that Defendant would safeguard Plaintiffs and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous 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 Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it 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 FTC Act, 15 U.S.C. §

45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not 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 FTC Act, 15 U.S.C. § 45.

398. Defendant's inadequate data security had no countervailing benefit to consumers or to competition. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

399. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous.

400. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiffs' and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

401. Defendant's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

402. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

403. Plaintiffs and the Class Members seek relief under Colo. Rev. Stat. § 6-1-101 including, but not limited to injunctive relief, compensatory damages,

restitution, statutory damages, penalties, and attorneys' fees and costs.

FOURTEENTH CAUSE OF ACTION
Violation of the Maine Uniform Deceptive Trade Practices Act
10 Me. Rev. Stat. § 1212, *et seq*.
(On Behalf of Plaintiff McPhail and the Maine Subclass)

404. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein and bring this claim on behalf of themselves and the Nationwide Class, or, alternatively, Plaintiff McPhail and the Maine Subclass.

405. Defendant engaged in unlawful, unfair, and deceptive acts and practices, with respect to the sale and advertisement of the services paid for by Plaintiffs and the Class members, in violation of 5 Me. Rev. Stat. § 1212(E), (G), including by representing that Defendant would adequately protect Plaintiffs' and the Class members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous 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 Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it 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 FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not 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 FTC Act, 15 U.S.C. § 45.

406. Defendant's inadequate data security had no countervailing benefit to consumers or to competition. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

407. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous.

408. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiffs' and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

409. Defendant's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

410. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

411. Plaintiffs and the Class Members seek relief under 5 Me. Rev. Stat. § 1213, including but not limited to injunctive relief and attorneys' fees and costs.

FIFTEENTH CAUSE OF ACTION
Violation of the North Carolina Unfair Trade Practices Act N.C. Gen. Stat. An. § 75-1.1, *et seq*.
(On Behalf of Plaintiff Beckwith and the North Carolina Subclass)

412. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein and bring this claim on behalf of themselves and the Nationwide Class, or, alternatively, Plaintiff Beckwith and the North Carolina Subclass.

413. Defendant's sale, advertising, and marketing of home loan services affected commerce, as meant by N.C. Gen. Stat. § 75-1.1.

414. Defendant engaged in unlawful, unfair, and deceptive acts and practices, with respect to the sale and advertisement of the services paid for by Plaintiffs and the Class members, in violation of N.C. Gen. Stat. § 75-1.1, including by representing that Defendant would adequately protect Plaintiffs' and the Class members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks,

remediate identified security and privacy risks, and adequately improve security and privacy measures following previous 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 Plaintiffs and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it 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 FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not 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 FTC Act, 15 U.S.C. § 45.

415. Defendant's inadequate data security had no countervailing benefit to consumers or to competition. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

416. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous.

417. Defendant knew or should have known that its network and data security practices were inadequate to safeguard Plaintiffs' and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

418. Defendant's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class Members.

419. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

420. Plaintiffs and the Class Members seek relief under N.C. Gen. Stat. Ann. §§ 75-16 and 75-16.1, including, but not limited to injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

SIXTEENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class Against Defendant)

421. Plaintiffs re-allege and incorporate by reference all other paragraphs of this complaint as though fully set forth herein.

422. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

423. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to

safeguarding the data of Plaintiffs and the Class. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

424. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

425. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the Private Information it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

426. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

427. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

428. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its customers' (i.e., Plaintiffs and Class Members') data.

429. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are

not legally quantifiable or provable.

430. An injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

IX. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

1. For an Order certifying the proposed Class and any appropriate Subclasses, pursuant to California Civil Code Section 382, requiring notice thereto to be paid by Defendant and appointing Plaintiffs and their counsel to represent the Class(es);
2. For appropriate injunctive relief and/or declaratory relief, including, but not limited to, an order requiring Defendant to immediately secure and fully encrypt all confidential information, to store any computer passwords in a location separate from the computers, to cease negligently storing, handling, and securing their customers' confidential information, to notify customers whose Private Information was wrongly disclosed in an expedient and timely manner and to provide identity theft monitoring for an additional five years;
3. Adjudging and decreeing that Defendant has engaged in the conduct alleged herein;
4. For compensatory and general damages according to proof of certain causes of action;
5. For statutory damages on certain causes of action, including, but not limited to, statutory damages under the CCPA in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater, and all other damages available by statute or law;

6. For reimbursement, restitution and disgorgement on certain causes of action;

7. For both pre and post-judgment interest at the maximum allowable rate on any amounts awarded;

8. For costs of the proceedings herein;

9. For reasonable attorneys' fees, as allowed by statute; and

10. For any and all such other and further relief that this Court may deem just and proper, including, but not limited to, punitive or exemplary damages.

Dated: June 3, 2024

/s/ Daniel S. Robinson
Daniel S. Robinson
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, California
(949) 720-1288; Fax: (949) 720-1292
drobinson@robinsonfirm.com

/s/ Tina Wolfson
Tina Wolfson
AHDOOT & WOLFSON, PC
2600 W Olive Ave, Ste 500
Burbank, California 91505
(310) 474-9111; Fax: (310) 474-8585
twolfson@ahdootwolfson.com

/s/ Abbas Kazerounian
Abbas Kazerounian
KAZEROUNI LAW GROUP, APC
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
(800) 400-6808; Fax: (800) 520-5523
ak@kazlg.com

/s/ Stephen G. Larson
Stephen G. Larson
LARSON, LLP
555 S. Flower Street, 30th Floor
Los Angeles, CA 90071
(213) 436-4864; Fax: (213) 623-2000
slarson@larsonllp.com

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
(866) 252-0878

Interim Co-Lead Counsel for Plaintiffs

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues in this action so triable of right.

Dated: June 3, 2024

/s/ Daniel S. Robinson
Daniel S. Robinson
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, California
(949) 720-1288; Fax: (949) 720-1292
drobinson@robinsonfirm.com

/s/ Stephen G. Larson
Stephen G. Larson
LARSON, LLP
555 S. Flower Street, 30th Floor
Los Angeles, CA 90071
(213) 436-4864; Fax: (213) 623-2000
slarson@larsonllp.com

/s/ Tina Wolfson
Tina Wolfson
AHDOOT & WOLFSON, PC
2600 W Olive Ave, Ste 500
Burbank, California 91505
(310) 474-9111; Fax: (310) 474-8585
twolfson@ahdootwolfson.com

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
(866) 252-0878

/s/ Abbas Kazerounian
Abbas Kazerounian
KAZEROUNI LAW GROUP, APC
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
(800) 400-6808; Fax: (800) 520-5523
ak@kazlg.com

Interim Co-Lead Counsel for Plaintiffs