IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Case No. 25-cv-00692-PAB-NRN

(Consolidated with Civil Case Nos. 25-cv-00698-PAB-NRN, 25-cv-00728-PABNRN, 25-cv-00819-PAB-NRN, and 25-cv-00937-KAS)

Civil Case No. 25-cv-00692-PAB-NRN

MICHELLE O'LEARY, on behalf of herself and all others similarly situated,

Plaintiff,

v.

YES COMMUNITIES, LLC,

Defendant.

Civil Case No. 25-cv-00698-PAB-NRN

TERRY WILKINS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

YES COMMUNITIES, LLC,

Defendant.

Civil Case No. 25-cv-00728-PAB-NRN

TERESA STARKS, on behalf of herself and all others similarly situated,

Plaintiff,

v.

YES COMMUNITIES, LLC,

Defendant.

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Civil Case No. 25-cv-00819-PAB-NRN

BRENTON KAY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

YES COMMUNITIES, LLC,

Defendant.

Civil Case No. 25-cv-00937-KAS

JASMIN BURNS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

YES COMMUNITIES, LLC.

Defendant.

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Michelle O'Leary, Terry Wilkins, Teresa Starks, Brenton Kay, and Jasmin Burns, on behalf of and all others similarly situated, state as follows for their class action complaint against Defendant, Yes Communities, LLC, ("Yes Communities" or "Defendant"):

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and similarly situated Class Members' sensitive personally identifiable information ("PII"), which, as a result, has been wrongfully disclosed to cyberthieves.

2. In December 2024, hackers targeted and accessed Defendant's network systems through and stole Plaintiffs' and Class Members' sensitive, confidential PII stored therein,

including their full names in combination with their addresses, Social Security numbers, driver's license or state-issued ID numbers, and financial account information.

3. Plaintiffs and Class Members are current and former customers of Defendant who are Data Breach victims. In order to obtain housing from Defendant, Plaintiffs and Class Members were and are required to entrust Defendant with their sensitive, non-public PII. Defendant could not perform its operations or provide its services without collecting Plaintiffs' and Class Members' PII and retains it for many years, at least, even after the customer relationship has ended.

4. Yes Communities is a company headquartered in Colorado that owns mobile home communities in 23 states across the country.[1] Upon information and belief, the Data Breach has impacted thousands of consumers whose data was in Yes Communities' possession.

5. Businesses like Defendant that handle PII owe the individuals to whom that data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of PII to unauthorized persons—especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their private financial matters.

6. According to Defendant's Breach Notice the Data Breach lasted from December 9, 2024, to December 11, 2024. Defendant waited until February 24, 2025—over two months after

[1] *See Join Our Community*, YES COMMUNITIES, https://www.yescommunities.com/ (last visited March 3, 2025); *Community Portals,* YES COMMUNITIES https://www.yescommunities.com/Resident-Portal (last visited March 3, 2025).

the Data Breach first occurred—before it finally began notifying Class Members about the Data Breach ("Breach Notice").[2]

7. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering it an easy target for cybercriminals.

8. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell consumers how many people were impacted, how the breach happened, or why it took the Defendant over two months to finally begin notifying victims that cybercriminals had stolen their highly private information.

9. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect the PII in its possession, adequately notify impacted individuals of the Data Breach, and by obfuscating the nature of the Data Breach, Defendant violated state law and harmed an unknown number of consumers.

[2] Defendant's Breach Notice, addressed to and received by Plaintiff Teresa Starks, is attached hereto as **Exhibit A.**

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

12. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's PII due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

13. Plaintiffs and Class Members seek damages and equitable relief requiring Defendant to (a) disclose the full nature of the Data Breach and types of PII exposed; (b) implement data security practices to reasonably guard against future breaches; and (c) provide, at Defendant's expense, all Data Breach victims with lifetime identity theft protection services.

PARTIES

14. Plaintiff Michelle O'Leary ("Ms. O'Leary") is a natural person and citizen of Ohio, where she intends to remain. Ms. O'Leary is a Data Breach victim, receiving Yes Communities' Breach Notice dated February 24, 2025.

15. Plaintiff Terry Wilkins ("Mr. Wilkins") is a natural person and citizen of Florida, residing in Duval County, Florida where he intends to remain. Mr. Wilkins is a Data Breach victim, receiving Yes Communities' Breach Notice dated February 24, 2025.

16. Plaintiff Teresa Starks ("Ms. Starks"), is a natural person and citizen of Michigan, residing in Lexon, Michigan, where she intends to remain. Ms. Starks is a Data Breach victim, receiving Yes Communities' Beach Notice on or around March 3, 2025.

17. Plaintiff Brenton Kay ("Mr. Kay") is a natural person and citizen of Michigan, residing in Kalamazoo County, Michigan, where he intends to remain. Mr. Wilkins is a Data Breach victim, having received Yes Communities' Breach Notice on or around March 10, 2025.

18. Plaintiff Jasmin Burns ("Ms. Burns") is a natural person and citizen of North Carolina, residing in Greensboro, North Carolina, where she intends to remain. Ms. Burns is a Data Breach victim, receiving Yes Communities' Breach Notice dated February 24, 2025.

19. Defendant, Yes Communities, LLC, is a limited liability company organized under Delaware law with its headquarters and principal place of business located at 5050 S Syracuse Street, Suite 1200, Denver, Colorado 80237.

JURISDICTION & VENUE

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

21. Yes Communities is incorporated in Delaware and maintains its principal place of business in Colorado at 5050 S. Syracuse Street, Suite 1200, Denver, Colorado 80237. Yes Communities is therefore a Delaware and Colorado citizen.

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

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1)–(d) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

BACKGROUND FACTS

Yes Communities Owed Duties to Adopt Reasonable Data Security Measures for PII.

24. Yes Communities is a real estate company that builds, sells, finances and rents manufactured housing in communities located in 23 states,[3] with "major concentrations in Florida, Georgia, Iowa, Michigan, North Carolina, Oklahoma, South Carolina, Tennessee and Texas and continue[s] to grow."[4]

25. Plaintiffs and Class Members are current and former customers of Defendant who received housing and related services from Defendant on or prior to December 11, 2024.

26. As a condition of receiving housing and related services from Defendant, Defendants' customers, including Plaintiffs and Class Members, were required to entrust Defendant with highly sensitive PII, including their names, Social Security numbers, driver's license numbers, and other sensitive data.

27. In exchange for receiving Plaintiffs' and Class Members' PII, Defendant promised to safeguard the sensitive, confidential data and use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

28. The information Defendant held in its computer networks at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

---

[3] *See Join Our Community,* YES COMMUNITIES, https://www.yescommunities.com/ (last visited Mar. 6, 2025).

[4] *Our Communities*, YES COMMUNITIES, https://www.yescommunities.com/About/Our-Communities (last visited Mar. 6, 2025).

29. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive PII belonging to Plaintiffs and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

30. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial matters.

31. Yes Communities understood the need to protect the PII in its possession and prioritize data security, and made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them as a condition of obtaining housing and services from Defendant would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it were no longer required to maintain it.

32. Indeed, Defendant states in its Privacy Policy that it is "committed to protecting Your privacy and delivering a safe online experience;" that it "secures Your Personal Information from unauthorized access, use or disclosure;" and that it "secures the Personal Information You provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When Personal Information (such as a credit card number) is transmitted to other Web sites, it is protected through the use of encryption, such as the Secure Socket Layer (SSL) protocol."[5]

[5] *Yes! Communities Privacy Polity,* YES COMMUNITIES, https://www.yescommunities.com/Privacy-Policy (last visited Mar. 6, 2025).

33. Plaintiffs and Class Members relied on these promises from Defendant, a sophisticated financial institution, to implement reasonable practices to keep their sensitive PII confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete PII from Defendant's systems when no longer necessary for its legitimate business purposes.

34. But for Defendant's promises to keep Plaintiffs' and Class Members' PII secure and confidential, Plaintiffs and Class Members would not have sought services from or entrusted their PII to Defendant. Consumers in general demand security to safeguard their PII, especially when sensitive financial information is involved.

35. Based on the foregoing representations and warranties and to obtain services from Defendant, Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and protected against unauthorized access.

36. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII. To that end, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

37. Defendant derived economic benefits from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform its operations of hiring and deploying staffers or furnish the services it provides. 45. Additionally, Defendant benefits from collecting Plaintiffs' and Class Members' PII by using it for analytics and marketing purposes.

38. By obtaining, using, and benefiting from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting that PII from unauthorized access and disclosure.

39. Defendant had and has a duty to adopt reasonable measures to keep Plaintiffs' and Class Members' PII confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its IT networks, and train employees with access to use adequate cybersecurity measures.

40. Defendant had and has obligations created by the FTC Act, 15 U.S.C. § 45, common law, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and protected from unauthorized disclosure.

41. Despite its promises to secure the PII in its possession and its recognition of its duty to protect the PII in its care, on information and belief, Yes Communities has not implemented reasonably cybersecurity safeguards or policies to protect its employees' and residents' PII or train its employees to prevent, detect, and stop breaches of its systems. As a result, Yes Communities leaves significant vulnerabilities in its systems for cybercriminals to access and steal the PII in its possession.

Yes Communities' Failed to Adequately Safeguard Plaintiffs' and the Class Members' PII, Causing the Data Breach

42. Between December 9, 2024 and December 11, 2024, Defendant was hacked.[6]

43. According to Defendant, it "became aware of suspicious activity within [its] network and immediately took steps to investigate the activity and verify the security of [its] network."[7]

[6] *See* Exhibit A.
[7] *Id.*

44. Defendant stated it launched an investigation, which alarmingly, revealed that "there was unauthorized access to our network between December 9, 2024, and December 11, 2024, and during this time *files were copied*."[8]

45. Defendant further reported to the Iowa Attorney General that its investigation "identified ransomware on certain Yes Communities systems."[9]

46. According to the United States' Cybersecurity and Infrastructure Security Agency ("CISA"), ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.[10] Malicious actors then demand ransom in exchange for decryption, often threatening to sell or leak exfiltrated data or authentication information if the ransom is not paid.[11]

47. Defendant admitted that the following PII stolen by the ransomware actor included:

a. names;

b. Social Security numbers;

c. driver's license numbers; and,

d. financial account information.

48. Due to the obfuscating language in Defendant's Breach Notice and "Notice of Data Event," the extent of the ransomware actor's "access" to its systems and what PII of Plaintiffs' and the Class was "copied" is unknown.[12] It is also unknown how the ransomware actor was able to gain "access" to Defendant's computer network or how many of Yes Communities employees and

[8] *Id.*
[9] Defendant's "Notice of Data Event" sent to the Iowa Attorney General is attached hereto as **Exhibit B**.
[10] *Ransomware FAQs*, CISA, https://www.cisa.gov/stopransomware/ransomware-faqs (last visited Mar. 6, 2025).
[11] *Id.*
[12] *See id.*

residents, and/or possibly others, were impacted by the Data Breach. Additionally, Defendant failed to explain with any specificity what remedial measures it has undertaken to ensure such a breach does not occur again.

49. Thus, Defendant's purported 'disclosure' amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

50. To make matters worse, although the Data Breach occurred between December 9, 2024, and December 11, 2024, Defendant waited until February 24, 2025, before it began notifying the Class. **Exhibit A.** Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

51. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors;"

b. "As an added precaution, we are offering you access to 12 months of complimentary credit monitoring and identity protection services." *Id.*

52. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from stealing the PII in its possession. Thus, Defendant caused widespread injury and monetary damages.

53. Since the breach, Defendant vaguely states it is "implementing additional security measures within [its] network and [is] completing a review of [its] policies and procedures to further secure the information in [its] systems." *Id.* But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

54. Moreover, Defendant has not explained what "additional security measures within [its] network" actually entails. Thus, upon information and belief, Plaintiffs' and Class Members' PII remains unsecure.

55. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese – by sending a notice of data breach letter to Plaintiffs and Class Members, it admits that it has a reasonable belief that Plaintiffs' and Class Members' names and Social Security numbers were accessed or acquired by an unknown actor – aka cybercriminals.

56. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' Social Security numbers for download and theft.

57. Defendant could have prevented this Data Breach by properly training personnel,

securing account access through measures like phishing-resistant (i.e., non-SMS text based) multifactor authentication ("MFA") for as many services as possible, training users to recognize and report phishing attempts, implementing recurring forced password resets, and/or securing and encrypting files and file servers containing Plaintiffs' and Class Members' PII, but failed to do so.

58. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive PII it collected and maintained from Plaintiffs and Class Members, such as phishing-resistant MFA, standard monitoring and altering techniques, encryption, or deletion of information when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network, access it through Defendant's employee email account, and exfiltrate files containing Plaintiffs and Class Member's PII.

59. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' PII, using controls like limitations on personnel with access to sensitive data and requiring phishing-resistant MFA for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access. Defendant would have recognized the malicious activities if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

60. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

61. Because of Defendant's Data Breach, the sensitive PII of Plaintiffs and Class

members was placed into the hands of cybercriminals—causing Plaintiffs' and the Class's PII to be stolen and put up sale on the dark web.

62. Indeed, ransomware groups often post links to stolen data on a Data Leak Site ("DLS").[13] A DLS is a "website where the illicitly retrieved data of companies, that refuse to pay the ransom, are published."[14]

63. However, even if a ransomware group removes stolen data from its DLS when a ransom is paid, there is no guarantee that the data will be deleted. The stolen PII is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.[15]

64. Ransomware groups can therefore monetize stolen PII and sell it on the dark web as part of a full identity profile.[16] Buyers can then use that information to conduct different types of identity theft or fraud, such as to file a fake tax return, to apply for a fraudulent mortgage or to open a bank account while impersonating the victim.[17]

65. Thus, on information and belief, Plaintiffs' and the Class's PII has already been published, or will be published imminently, on the dark web.

---

[13] Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, HIPAA JOURNAL (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/#:~:text=While%20ransomware%20groups%20usually%20remove,little%20incentive%20to%20delete%20it.

[14] *Dedicated Leak Sites (DLS): Here's what you should know*, GROUP-IB, https://www.group-ib.com/resources/knowledge-hub/dedicated-leak-sites/ (last visited Feb. 5, 2025).

[15] *Id.*

[16] Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, MALICIOUSLIFE BY CYBEREASON, https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion (listed visited Mar. 6, 2025).

[17] *Id.*

66. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

67. On information and belief, Yes Communities failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' and residents' PII. Defendant's negligence is evidenced by its failure to promptly detect the Data Breach, prevent the Data Breach, and stop cybercriminals from stealing the PII.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

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

69. Defendant's negligence in failing to safeguard Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing such data. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business, should have known that the PII it collected and maintained would be vulnerable to and targeted by cybercriminals.

70. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry. Those 330 reported breaches

exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

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

72. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[18]

73. As a business in possession of its current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

74. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being wrongfully disclosed to cybercriminals.

75. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' PII compromised therein would be targeted by hackers and cybercriminals for use in

[18] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Feb. 9, 2024).

variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

76. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to at least tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

77. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

78. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and the like.

Defendant Could Have Prevented the Data Breach

79. Data breaches are preventable.[19] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[20] She added that "[o]rganizations that collect, use, store, and share sensitive personal

[19] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[20] *Id.* at 17.

data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[21]

80. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [22]

81. In a Data Breach like the one here, many failures laid the groundwork for the Breach.

82. For example, the FTC has published guidelines that establish reasonable data security practices for businesses. The guidelines also emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

83. Additionally, several industry-standard best practices have been identified that—at a minimum—should be implemented by businesses like Defendant.

Defendant Failed to Follow FTC Guidelines

84. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

[21] *Id.* at 28.
[22] *Id.*

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business. There, the FTC set guidelines for what data security principles and practices businesses must use. The FTC declared that, inter alia, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

86. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

87. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

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

89. In short, Defendant's failure to use reasonable and appropriate measures to protect against the unauthorized acquisition of its current and former employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Comply with the GLBA

90. The GLBA states, "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

91. Defendant is a financial institution for purposes of the GLBA, because it is "significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities," 16 C.F.R. § 314.2(h), in leasing, selling, and financing residential real estate.

92. "Nonpublic personal information" means "personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A)(i)–(iii).

93. The PII involved in the Data Breach constitutes "nonpublic personal information" for purposes of the GLBA.

94. Defendant collects "nonpublic personal information," as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) & 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801, et seq., and to numerous rules and regulations promulgated under the GLBA.

95. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (i) designating one or more employees to coordinate the information security program; (ii) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (iii) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (iv) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (v) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 & 314.4. As alleged herein, Defendant violated the Safeguards Rule.

96. Defendant's conduct resulted in a variety of failures to follow GLBA-mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Defendant failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its information technology systems.

97. Had Defendant implemented data security protocols, the consequences of the Data Breach could have been avoided, or at least significantly reduced as the Data Breach could have been detected earlier, the amount of PII compromised could have been greatly reduced.

Defendant Failed to Comply with Industry Standards

98. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

99. Other industry standard best practices 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.

100. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), the Center for Internet Security's Critical Security Controls (CIS CSC), and the Cybersecurity & Infrastructure Security Agency ("CISA"), which are all established standards in reasonable cybersecurity readiness.

101. The NIST recommends certain practices to safeguard systems:[23]

a. Control who logs on to your network and uses your computers and other devices.

[23] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist- framework (last acc. Feb. 9, 2024).

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity.

102. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[24]

103. Further still, the Cybersecurity & Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known

[24] See Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[25]

104. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Plaintiff Michelle O'Leary's Experiences and Injuries

105. Plaintiff Michelle O'Leary is a former customer of Defendant and received housing and related services from Defendant prior to the Data Breach. Plaintiff provided her PII to Defendant as a condition of and in exchange for obtaining housing and related services from Defendant.

106. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network systems with inadequate data security (despite the fact she is a former customer of Defendant) causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

107. Plaintiff reasonably believed her sensitive information would be deleted from Defendant's computer systems once she ceased being a customer of Defendant. It was not.

[25] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Feb. 9, 2024).

108. Plaintiff received Defendant's Breach Notice dated February 24, 2025, notifying her that her PII was accessed by and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including her name and Social Security number.

109. The Notice offered Plaintiff only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information. Therefore, Plaintiff has a continuing interest in securing lifetime identity theft protection services.

110. Plaintiff greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

111. Plaintiff would not have provided her PII to Defendant had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

112. Defendant had the duty and obligation to use reasonable measures to protect the PII in its possession according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized theft and disclosure.

113. On information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

114. Plaintiff has spent—and will continue to spend—significant time and effort to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or

attempted identity theft or fraud. Plaintiff now regularly monitors her financial and credit statements and has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

115. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

116. The risk of identity theft is imminent, impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff further believes her PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

117. Plaintiff suffered actual injury from the exposure and theft of her PII and its threatened or actual publication on the dark web—which violates her rights to privacy.

118. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach. This is compounded by the fact that Defendant still has not fully informed her of the key details about the Data Breach's occurrence or the information stolen.

119. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

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

121. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its residents' Private Information.

Plaintiff Terry Wilkins Experiences and Injuries

122. Plaintiff Terry Wilkins is a former customer of Defendant and received housing and related services from Defendant prior to the Data Breach. Plaintiff provided his PII to Defendant as a condition of and in exchange for obtaining housing and related services from Defendant.

123. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network systems with inadequate data security (despite the fact he is a former customer of Defendant) causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

124. Plaintiff reasonably believed his sensitive information would be deleted from Defendant's computer systems once he ceased being a customer of Defendant. It was not.

125. Plaintiff received Defendant's Breach Notice dated February 24, 2025, notifying him that his PII was accessed by and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including his name, driver's license number, and Social Security number.

126. The Notice offered Plaintiff only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information. Therefore, Plaintiff has a continuing interest in securing lifetime identity theft protection services.

127. Plaintiff greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

128. Plaintiff would not have provided his PII to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

129. Defendant had the duty and obligation to use reasonable measures to protect the PII in its possession according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized theft and disclosure.

130. On information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

131. On information and belief, Plaintiff's phone number was exfiltrated from Defendant's systems by a ransomware group in the Data Breach. Indeed, in the aftermath of the Data Breach, Plaintiff has been bombarded with spam phone calls.

132. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from him and committing identity theft by way of a phishing attack or social engineering attack.

133. Plaintiff has spent—and will continue to spend—significant time and effort to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors his financial and credit statements multiple times a week and has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

134. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

135. The risk of identity theft is imminent, impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff further believes his PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

136. Plaintiff suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

137. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach. This is compounded by the fact that Defendant still has not fully informed his of the key details about the Data Breach's occurrence or the information stolen.

138. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

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

140. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its residents' Private Information.

Plaintiff Teresa Starks' Experiences and Injuries

141. Plaintiff Teresa Starks is a former employee of Defendant, having worked for Yes Communities from 2023 to 2025. Defendant used Plaintiff's PII to facilitate its business.

142. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network systems with inadequate data security (despite the fact she is a former employee of Defendant) causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

143. Plaintiff reasonably believed her sensitive information would be deleted from Defendant's computer systems once her business relationship with Defendant ended. It was not.

144. Plaintiff received Defendant's Breach Notice on or around March 3, 2025, notifying her that her PII was accessed by and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including her name, Social Security number, and driver's license number.

145. The Notice offered Plaintiff only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information. Therefore, Plaintiff has a continuing interest in securing lifetime identity theft protection services.

146. Plaintiff greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

147. Plaintiff would not have provided her PII to Defendant had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

148. Defendant had the duty and obligation to use reasonable measures to protect the PII in its possession according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized theft and disclosure.

149. On information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

150. On information and belief, Plaintiff's phone number was exfiltrated from Defendant's systems by a ransomware group in the Data Breach. Indeed, in the aftermath of the Data Breach, Plaintiff has been bombarded with spam phone calls. Plaintiff continues to actively block spam calls, yet continues to receive new spam communications daily.

151. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a social engineering attack.

152. Plaintiff has spent—and will continue to spend—significant time and effort to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Additionally, Plaintiff has placed a lock on her debit and credit cards, so that she must affirmatively unlock each card before she attempts to use it. And Plaintiff now regularly monitors her financial and credit statements and has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

153. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

154. The risk of identity theft is imminent, impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff further believes her PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

155. Plaintiff suffered actual injury from the exposure and theft of her PII and its threatened or actual publication on the dark web—which violates her rights to privacy.

156. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach. This is compounded by the fact that Defendant still has not fully informed her of the key details about the Data Breach's occurrence or the information stolen.

157. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

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

159. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its residents' Private Information.

Plaintiff Brenton Kay's Experiences and Injuries

160. Plaintiff Brenton Kay applied to receive housing and related services from Defendant prior to the Data Breach. Plaintiff provided his PII to Defendant as a condition of and in exchange for potentially obtaining housing and related services from Defendant.

161. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network systems with inadequate data security causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

162. Plaintiff reasonably believed his sensitive information would be deleted from Defendant's computer systems once he ceased being a customer of Defendant. It was not.

163. Plaintiff received Defendant's Breach Notice around March 10, 2025, notifying him that his PII was accessed by and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including his name, driver's license number, and Social Security number.

164. The Notice offered Plaintiff only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information. Therefore, Plaintiff has a continuing interest in securing lifetime identity theft protection services.

165. Plaintiff greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

166. Plaintiff would not have provided his PII to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

167. Defendant had the duty and obligation to use reasonable measures to protect the PII in its possession according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized theft and disclosure.

168. On information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

169. On information and belief, Plaintiff's phone number was exfiltrated from Defendant's systems by a ransomware group in the Data Breach. Indeed, in the aftermath of the Data Breach, Plaintiff has been bombarded with spam phone calls. Specifically, he has been

receiving a combination of around 5-6 spam calls or texts, and many spam emails per day. Prior to this time, he was receiving maybe one troublesome call and/or email per day.

170. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from him and committing identity theft by way of a phishing attack or social engineering attack.

171. Plaintiff has spent—and will continue to spend—significant time and effort to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors his financial and credit statements multiple times a week and spends at minimum forty minutes per week in an effort to mitigate the damage that has been caused by the Data Breach, valuable time he otherwise would have spent on other activities. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

172. Plaintiff signed up for credit monitoring through Equifax, and further anticipates spending considerable money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

173. The risk of identity theft is imminent, impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff further believes his PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

174. Plaintiff suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

175. Plaintiff suffered further actual injury as he has been the victim of identity theft since the Data Breach occurred. He received a bill for a Sprint account that he did not open. He also learned that an authorized person applied for a loan using his PII through Alliance Financial. He secures his data in a safe manner and has not experienced fraud before or in recent years. Plaintiff Kay logically believes this is related to the Data Breach given the timeline and nature of the incident.

176. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach. This is compounded by the fact that Defendant still has not fully informed his of the key details about the Data Breach's occurrence or the information stolen.

177. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. He is very concerned about his credit and loans being taken out in his name by others. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

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

179. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its residents' Private Information.

Plaintiff Jasmin Burns Experiences and Injuries

180. Plaintiff Jasmin Burns is a former employee of Defendant. Plaintiff provided her PII to Defendant as a condition of and in exchange for obtaining employment services from Defendant.

181. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network systems with inadequate data security (despite the fact she is a former customer of Defendant) causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

182. Plaintiff reasonably believed her sensitive information would be deleted from Defendant's computer systems once she ceased being a customer of Defendant. It was not.

183. Plaintiff received Defendant's Breach Notice dated February 24, 2025, notifying her that her PII was accessed by and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including her name and Social Security number.

184. The Notice offered Plaintiff only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information. Therefore, Plaintiff has a continuing interest in securing lifetime identity theft protection services.

185. Plaintiff greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

186. Plaintiff would not have provided her PII to Defendant had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

187. Defendant had the duty and obligation to use reasonable measures to protect the PII in its possession according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized theft and disclosure.

188. On information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the dark web.

189. On information and belief, Plaintiff's email address and phone number were exfiltrated from Defendant's systems by a ransomware group in the Data Breach. Indeed, in the aftermath of the Data Breach, Plaintiff has been bombarded with spam phone calls, text messages, and emails.

190. Plaintiff is concerned that the spam calls, texts, and emails are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a phishing attack or social engineering attack.

191. Plaintiff has spent—and will continue to spend—significant time and effort to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now regularly monitors her financial and credit statements and has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

192. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

193. The risk of identity theft is imminent, impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff further believes her PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

194. Plaintiff suffered actual injury from the exposure and theft of her PII and its threatened or actual publication on the dark web—which violates her rights to privacy.

195. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach. This is compounded by the fact that Defendant still has not fully informed her of the key details about the Data Breach's occurrence or the information stolen.

196. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

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

198. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long

as Defendant fails to undertake the necessary and appropriate security and training measures to protect its residents' Private Information.

Plaintiffs and the Class Suffered Common Injuries and Damages Due to Defendant's Conduct

199. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' PII directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their PII in the Data Breach.

200. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, inter alia, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. identity theft and fraud;

b. loss of time to mitigate the risk of identity theft and fraud;

c. diminution in value of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud;

e. lost benefit of the bargain and opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, inter alia, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

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

h. compromise and continuing publication of their PII;

i. unauthorized use of their stolen PII;

j. invasion of privacy; and

k. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

Risk of Continued Identity Theft

201. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

202. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

203. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." Id.

204. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the dark web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

205. The dark web is an unindexed layer of the internet that requires special software or authentication to access.26 Criminals in particular favour the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web

[26] *What Is the Dark Web?,* Experian, available at https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/.

users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[27] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

206. The unencrypted PII of Plaintiff and Class Members has or will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

207. The value of Plaintiffs' and Class's PII on the black market is considerable. Stolen PII trades on the black market for years and is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

208. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

209. Because a person's identity is akin to a puzzle with multiple data points, 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 to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

[27] *Id.*

210. 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 Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

211. Identity thieves can also use an individual's personal data and PII 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 Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, 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 issued in the victim's name.[28]

212. One example of criminals piecing together bits and pieces of compromised PII to create comprehensive dossiers on individuals is called "Fullz" packages.[29] These dossiers are both

[28] *Identity Theft and Your Social Security Number,* Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[29] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, 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 off 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 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*

shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. For example, they can combine the stolen PII, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

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

214. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

215. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[31] Yet, Defendant failed to

---

Underground Stolen from Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

[30] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[31] *Id.*

rapidly report to Plaintiff and the Class that their PII was stolen. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

218. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

219. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

220. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office 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.

221. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

222. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

223. These efforts are consistent with the steps that FTC recommends that data breach 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 (consider an extended fraud alert that lasts for seven 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.[32]

224. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

[32] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

Diminished Value of PII

225. Personal data like PII is a valuable property right.[33]

226. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

227. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[34]

228. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.[36]

229. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

230. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now

---

[33] *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).
[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[35] *See* https://datacoup.com/ *and* https://digi.me/what-is-digime/.
[36] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

231. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

232. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

233. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

234. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information 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.

235. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[37]

236. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

[37] See Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds,* FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

237. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

238. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Lost Benefit of the Bargain

239. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

240. When agreeing to provide their PII, which was a condition precedent to obtain housing and related services from Defendant, Plaintiff and Class Members, as customers and consumers, understood and expected that they were, in part, paying for services and data security to protect the PII they were required to provide.

241. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

CLASS ACTION ALLEGATIONS

242. Plaintiffs bring this action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

243. Plaintiffs sue on behalf of themselves and the proposed Class ("Class"), defined as follows:

All individuals residing in the United States whose PII may have been compromised in Defendant's Data Breach, including all those who received Notice of the Data Breach.

244. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

245. Plaintiffs reserve the right to amend the class definition.

246. This action satisfies the numerosity, commonality, typicality, and adequacy requirements for suing as representative parties:

247. **Numerosity.** Plaintiffs are representative of the proposed Class, consisting of potentially thousands of members, far too many to join in a single action;

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

249. **Typicality.** Plaintiffs' claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

250. **Adequacy.** Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

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

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

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

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

d. Whether Defendant breached contract promises to safeguard Plaintiffs and the Class's Sensitive Information;

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

f. Whether Defendant's Breach Notice was reasonable;

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

h. What the proper damages measure is; and

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

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

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

253. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

254. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII and/or not disclose their PII to unauthorized third parties.

255. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

256. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

257. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII to facilitate its business.

258. Defendant owed to Plaintiffs and Class members at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized disclosure;

c. promptly detect attempts at unauthorized access; and

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII.

259. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

260. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

261. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

262. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their PII a necessary part of doing business with Defendant or being employed by Defendant.

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

264. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs' and Class members' and the importance of exercising reasonable care in handling it.

265. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

266. Defendant breached these duties as evidenced by the Data Breach.

267. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII by:

a. disclosing and providing access to this information to third parties;

b. failing to destroy or delete data belonging to individuals such as former employees and customers, even though Defendant that it did not have an ongoing customer relationship or business relationship with these individuals;

c. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

268. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

269. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries-in-fact.

270. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

271. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including

monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

272. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the dark web.

273. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

274. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

275. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

276. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class members' sensitive PII. As a result of Defendant's failure, the Sensitive Information of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their

Sensitive Information was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their Sensitive Information in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

277. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

278. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTC Act was intended to protect.

279. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class Members as a result of the Data Breach.

280. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

281. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its residents and/or its employees, which is recognized by laws and regulations including but not limited to Section 5 of the FCT Act,

as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

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

283. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

285. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

286. Had Plaintiffs and the Class known that Defendant would not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

287. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence per se.

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

289. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

290. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

291.

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

293. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

294. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

295. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

297. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

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

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

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

301. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiffs and the Class.

302. Plaintiffs, on behalf of herself and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Sensitive Information.

303. Plaintiffs, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV
Breach of Contract
(On behalf of Plaintiffs and the Class)

304. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

305. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Yes Communities in exchange for residential services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

306. Yes Communities' Privacy Policy memorialized the rights and obligations of Yes Communities and its residents. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

307. In the Privacy Policy, Yes Communities commits to protecting the privacy and security of private information in its possession from unauthorized access and disclosure.

308. Plaintiff and Class Members fully performed their obligations under their contracts with Yes Communities.

309. However, Yes Communities did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Yes Communities breached its contracts with Plaintiff and Class Members.

310. Yes Communities allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, Yes Communities breached the Privacy Policy with Plaintiff and Class Members.

311. Yes Communities' failure to satisfy its confidentiality and privacy obligations resulted in Yes Communities providing services to Plaintiff and Class Members that were of a diminished value.

312. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

313. As a direct and proximate result of Yes Communities' conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

314. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Yes Communities to, inter alia, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

315. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

316. Defendant offered to employ and/or provide housing and other services to Plaintiffs and members of the Class if, as a condition of that employment or of obtaining housing and other services, Plaintiffs and members of the Class provided Defendant with their PII.

317. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employees' and/or its residents' PII.

318. Plaintiffs and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment and/or housing and other services with Defendant.

319. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

320. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

321. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

322. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

323. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

324. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

325. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

326. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

327. In these and other ways, Defendant violated its duty of good faith and fair dealing.

328. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

329. Plaintiffs, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

330. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

331. This claim is pled in the alternative or in addition to other causes of action where necessary.

332. Plaintiffs and Class Members conferred a monetary benefit on Defendant conferred a benefit upon Defendant in the form of their labor and/or in the form of payments to Defendant for housing and other services. Defendant also benefited from the receipt of Plaintiffs' and the Class's PII, as this was used to facilitate their employment or to facilitate Defendant's business.

333. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Sensitive Information.

334. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

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

337. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have provided their PII to Defendant.

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

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

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

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

COUNT VII
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

342. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

343. 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 here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

344. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information.

345. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

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

a. Yes Communities continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Yes Communities' existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security

procedures and practices that are appropriate to protect residents' Private Information; and

c. Yes Communities continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

347. The Court also should issue corresponding prospective injunctive relief requiring Yes Communities to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information, including the following:

a. Order Yes Communities to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Yes Communities must implement and maintain reasonable security measures, including, but not limited to: (i) engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Yes Communities' systems on a periodic basis, and ordering Yes Communities to promptly correct any problems or issues detected by such third-party security auditors; (ii) engaging third-party security auditors and internal personnel to run automated security monitoring; (iii) auditing, testing, and training its security personnel regarding any new or modified procedures; (iv) segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Yes Communities' systems; (v) conducting regular database scanning and security checks; (vi) routinely and continually conducting 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 (vii) meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Yes Communities' residents should take to protect themselves.

348. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Yes Communities. The risk of another such breach is real, immediate, and substantial. If another breach at Yes Communities occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

349. The hardship to Plaintiff and class members if an injunction does not issue exceeds the hardship to Yes Communities if an injunction is issued. Among other things, if another massive data breach occurs at Yes Communities, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Yes Communities of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Yes Communities has a pre-existing legal obligation to employ such measures.

350. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Yes Communities, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

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

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Date: March 6, 2025

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
Samuel J. Strauss*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com
sam@straussborrelli.com

/s/Josh Sanford
Josh Sanford (Col. Bar No. 44358)
SANFORD LAW FIRM, PLLC
10800 Financial Center Pkwy, Suite 510
Little Rock, Arkansas 72211
Telephone: (501) 221-0088
josh@sanfordlawfirm.com

/s/Jarrett Ellzey
Jarrett Ellzey*
Leigh S. Montgomery*
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Telephone: (888) 350-3931
jellzey@eksm.com
lmontgomery@eksm.com
service only: service@eksm.com

/s/ Jeff Ostrow
Jeff Ostrow, Esq.
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

/s/ Gary E. Mason
Gary E. Mason
Danielle L. Perry
Lisa A. White
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

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

**Pro Hac Vice forthcoming*

Attorneys for Plaintiffs and Proposed Class

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that on May 15, 2025, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record via the ECF system.

DATED this 15th day of May, 2025.

STRAUSS BORRELLI PLLC

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

— EXHIBIT A —

Yes Communities, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PLFG0600104269
TERESA STARKS
[redacted]

February 24, 2025

PLFG0600104269042690104260400

Dear TERESA STARKS:

Yes Communities, LLC ("Yes Communities" or "we") is writing to inform you of an event which may involve some of your information. This letter provides an overview of the event, our response to the event, and steps you may take to protect your information, should you feel it is appropriate to do so.

What Happened? We became aware of suspicious activity within our network and immediately took steps to investigate the activity and verify the security of our network. The investigation determined there was unauthorized access to our network between December 9, 2024, and December 11, 2024, and during this time files were copied. We reviewed the files to determine the types of information present and to whom it relates, and on January 9, 2025, we completed the review.

What Information Was Involved? Our review of the involved files identified your name, and Social Security number and driver's license number.

What We Are Doing. We take this event and the security of personal information in our care seriously. Upon learning of the suspicious activity, we moved quickly to investigate and respond. The investigation included steps to assess and secure our network, review the involved files to determine what types of information may have been impacted, and notify potentially impacted individuals. As part of our ongoing commitment to the privacy of information, we are implementing additional security measures within our network and are completing a review of our policies and procedures to further secure the information in our systems. As an added precaution, we are offering you access to 12 months of complimentary credit monitoring and identity protection services. If you wish to activate these services, you may follow the instructions included in the *Steps You Can Take to Protect Personal Information* section on the next page of this letter. Please note you must enroll in these services directly, as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may review the *Steps You Can Take to Protect Personal Information* section of this letter for useful information on what you can do to better protect against possible misuse of information.

For More Information. If you have questions, you may contact us at 1-833-799-3904 from 8 a.m. to 8 p.m. Eastern Time, Monday through Friday, excluding US holidays.

Sincerely,

Yes Communities

— EXHIBIT B —

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 24, 2025

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Yes Communities, LLC ("Yes Communities") located at 5050 South Syracuse Street, Suite 1200, Denver, Colorado 80237, and are writing to notify your office of an event that may affect the security of personal information relating to six hundred forty-eight (648) Iowa residents (the "Event"). This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Yes Communities does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

Yes Communities became aware of suspicious activity within its network and promptly took steps to investigate the activity and verify the security of the network. The investigation determined there was unauthorized access to its network between December 9, 2024, and December 11, 2024, and during this time files were copied. The investigation also identified ransomware on certain Yes Communities systems. Yes Communities reviewed the files to determine the types of information present and to whom it relates. This effort recently concluded on January 9, 2025, and identified information relating to Iowa residents including name, Social Security number, drivers' license number, and financial account information.

Notice to Iowa Residents

On February 24, 2025, Yes Communities provided written notice of the Event to six hundred forty-eight (648) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the suspicious activity, Yes Communities moved quickly to investigate and respond. The investigation included steps to assess and secure the Yes Communities network, review the involved files, and identify potentially impacted individuals. Yes Communities notified federal law enforcement and is notifying relevant regulatory authorities. Yes Communities is implementing additional security measures within its network and is completing a review of its policies and procedures to further secure the information in its systems.

As noted above, Yes Communities is notifying individuals whose personal information may have been impacted by the Event. The notice letter includes access to complimentary credit monitoring services for twelve (12) months, through TransUnion and guidance on how to better protect against identity theft and fraud. Yes Communities is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the Event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/ogf
Enclosure

EXHIBIT A

Yes Communities, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

February 24, 2025

Dear

Yes Communities, LLC ("Yes Communities" or "we") is writing to inform you of an event which may involve some of your information. This letter provides an overview of the event, our response to the event, and steps you may take to protect your information, should you feel it is appropriate to do so.

What Happened? We became aware of suspicious activity within our network and immediately took steps to investigate the activity and verify the security of our network. The investigation determined there was unauthorized access to our network between December 9, 2024, and December 11, 2024, and during this time files were copied. We reviewed the files to determine the types of information present and to whom it relates, and on January 9, 2025, we completed the review.

What Information Was Involved? Our review of the involved files identified your name, and Social Security number.

What We Are Doing. We take this event and the security of personal information in our care seriously. Upon learning of the suspicious activity, we moved quickly to investigate and respond. The investigation included steps to assess and secure our network, review the involved files to determine what types of information may have been impacted, and notify potentially impacted individuals. As part of our ongoing commitment to the privacy of information, we are implementing additional security measures within our network and are completing a review of our policies and procedures to further secure the information in our systems. As an added precaution, we are offering you access to 12 months of complimentary credit monitoring and identity protection services. If you wish to activate these services, you may follow the instructions included in the *Steps You Can Take to Protect Personal Information* section on the next page of this letter. Please note you must enroll in these services directly, as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may review the *Steps You Can Take to Protect Personal Information* section of this letter for useful information on what you can do to better protect against possible misuse of information.

For More Information. If you have questions, you may contact us at 1-833-799-3904 from 8 a.m. to 8 p.m. Eastern Time, Monday through Friday, excluding US holidays.

Sincerely,

Yes Communities

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: . In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.