UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

COURTNEY GARNER, JERYL LUCIANI, and MICHAEL CRAIN, on behalf of themselves and a class of similarly situated persons,

Plaintiffs,

v.

AT&T, INC.,

Defendant.

NO.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Courtney Garner, Jeryl Luciani and Michael Crain, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendant AT&T, Inc. ("AT&T" or "Defendant"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclasses, as defined below. Plaintiffs make the following allegations upon information and belief, the investigation of their counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devasting. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have a grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

2. Dallas, Texas based AT&T markets itself as a sophisticated, reliable network provider that "take[s] cybersecurity very seriously and privacy is a fundamental commitment at AT&T."[2] AT&T represents: "We use strong safeguards to keep your data safe and secure."[3] and that at AT&T:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs.

[1] Dave Maxfield & Bill Latham, Data Breaches: Perspectives from Both Sides of the Wall, S.C. Lawyer (May 2014).

[2] *Keeping your account secure*, AT&T, https:// https://www.att.com/support/article/my-account/000101995?bypasscache=1/?source=EPcc000000000000U (last visited Apr. 4, 2024).

[3] *Our Privacy Approach.* AT&T, https://about.att.com/privacy.html (last visited Apr. 4, 2024).

> And we require callers and online users to authenticate themselves before we provide account information.[4]

3. Despite these representations, AT&T seems incapable of adequately protecting the information it maintains from and about its customers. Just last March (2023), AT&T notified nine million wireless customers that their account information had been exposed. In March of this year, it announced a far larger data breach that impacts 73 million of its customers (the "Data Breach").

4. What is extraordinarily troubling about the Data breach is that it did not stem from a recent intrusion. Rather, the Personally Identifying Information (PII) of some 7.6 million current AT&T customers and 65.4 million former AT&T customers was likely stolen in 2018, without AT&T ever detecting the intrusion or exfiltration of these huge amounts of data. This fact alone portends that AT&T's data security systems are woefully inadequate and at least negligently monitored and controlled.

5. Since the intrusion and exfiltration of the PII of 73 million AT&T customers there have been several listings, postings and descriptions of the pilfered data made available online and reported to AT&T, yet in each instance AT&T denied that its systems had been breached. Only in late March 2024, did AT&T finally admit this trove of PII came from its system and begin the process of notifying those tens of millions of affected consumers. All the while, hackers and criminals have had access to this valuable information, exposing affected consumers to severe risks of identity theft and financial fraud.

6. AT&T has admitted that hackers gained access to customer information and may have obtained "full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, AT&T account numbers, and passcodes.[5]

7. As a result of the Data Breach, through which their Personally Identifiable Information ("PII") was compromised, disclosed, and obtained by unauthorized third parties,

---

[4] *AT&T Privacy Notice*, https://about.att.com/privacy/privacy-notice.html#data-retention (last visited Apr. 4. 2024).

[5] *See supra,* N. 2..

Plaintiffs and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiffs and the other Class Members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

8. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

II. JURISDICTION, VENUE, AND CHOICE OF LAW

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

10. The Court has jurisdiction over Defendant AT&T, Inc. because AT&T, Inc. maintains its principal place of business in this District, has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because AT&T's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

A. Plaintiff Courtney Garner

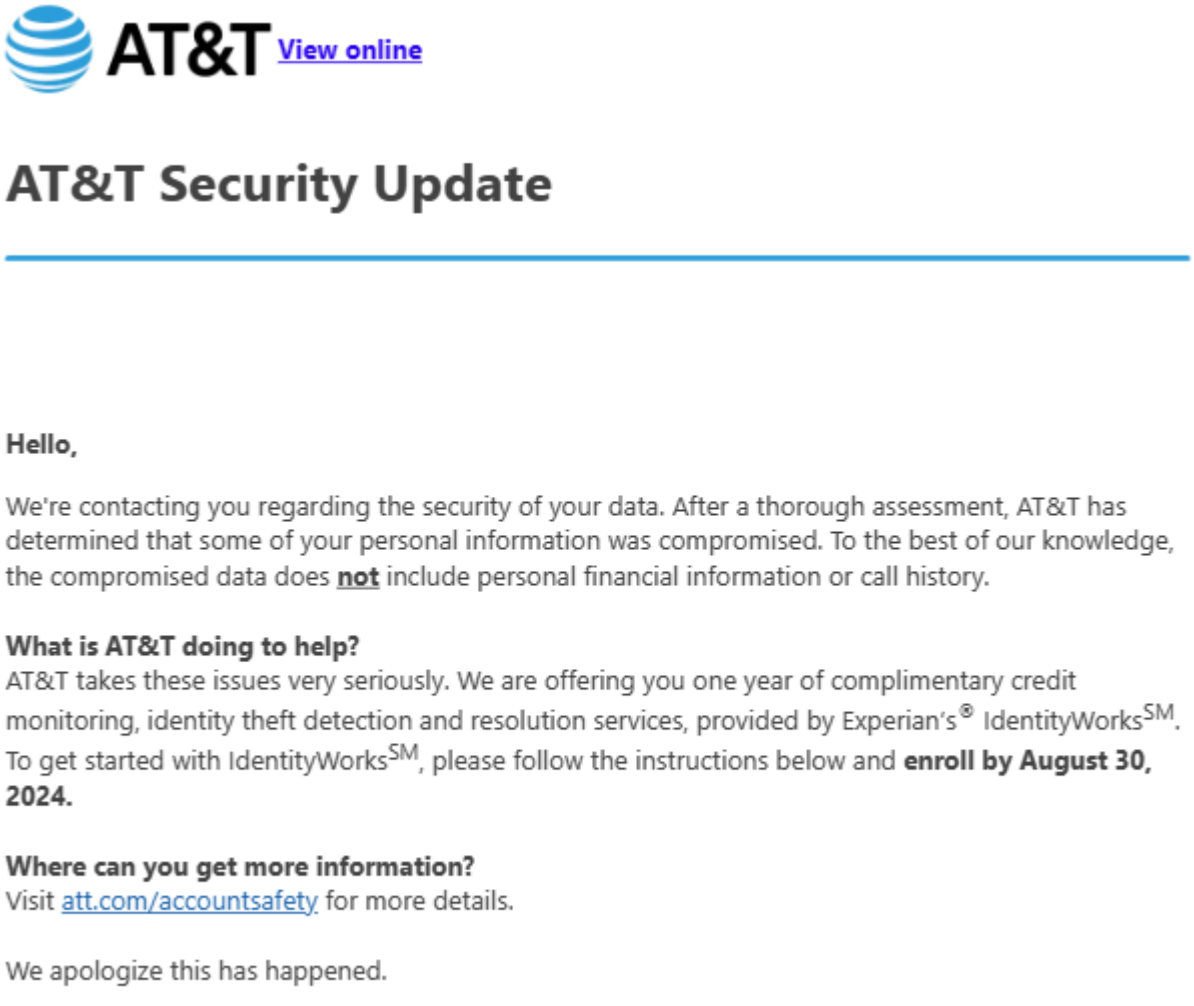
12. Plaintiff Courtney Garner is a citizen of and is domiciled in the state of Tennessee.

13. Plaintiff is a former customer of AT&T and used its cellular telephone services from approximately 2017 through 2021.

14. Plaintiff provided confidential and sensitive PII to AT&T, as requested and required by AT&T for the provision of its services. AT&T obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

15. Plaintiff would not have entrusted her PII to AT&T had she known that AT&T failed to maintain adequate data security.

16. On or about April 12, 2024, plaintiff received the following notification from AT&T that her information was compromised:



AT&T View online

AT&T Security Update

Hello,

We're contacting you regarding the security of your data. After a thorough assessment, AT&T has determined that some of your personal information was compromised. To the best of our knowledge, the compromised data does **not** include personal financial information or call history.

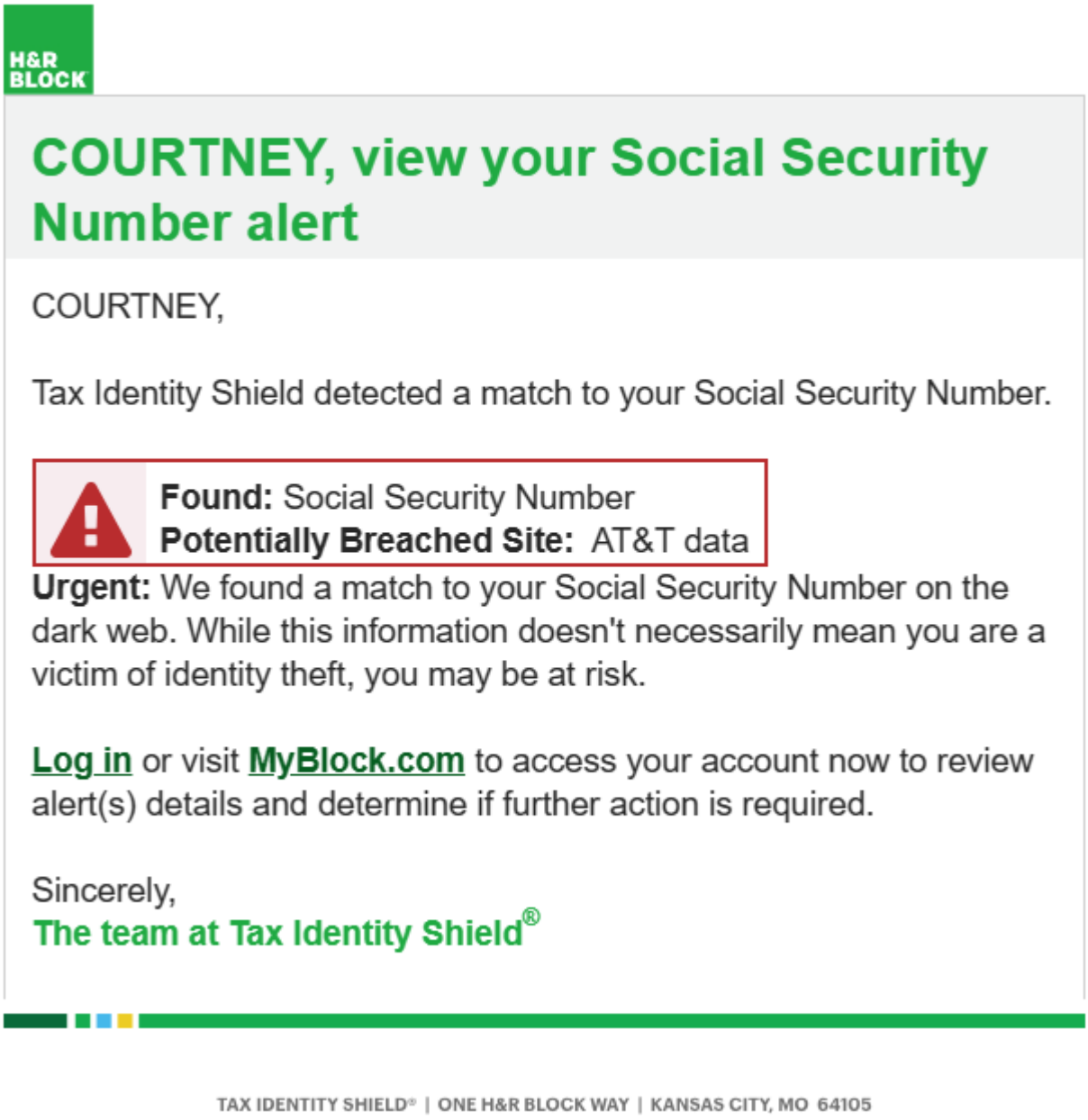
What is AT&T doing to help?
AT&T takes these issues very seriously. We are offering you one year of complimentary credit monitoring, identity theft detection and resolution services, provided by Experian's® IdentityWorks℠. To get started with IdentityWorks℠, please follow the instructions below and **enroll by August 30, 2024.**

Where can you get more information?
Visit att.com/accountsafety for more details.

We apologize this has happened.

AT&T

17. Shortly thereafter, Plaintiff also received the following notification from her H&R Block credit monitoring service that as a result of the Data Breach, Plaintiff's PII was available on the Dark Web:



H&R BLOCK

COURTNEY, view your Social Security Number alert

COURTNEY,

Tax Identity Shield detected a match to your Social Security Number.

Found: Social Security Number
Potentially Breached Site: AT&T data

Urgent: We found a match to your Social Security Number on the dark web. While this information doesn't necessarily mean you are a victim of identity theft, you may be at risk.

Log in or visit MyBlock.com to access your account now to review alert(s) details and determine if further action is required.

Sincerely,
The team at Tax Identity Shield®

TAX IDENTITY SHIELD® | ONE H&R BLOCK WAY | KANSAS CITY, MO 64105

18. Plaintiff also received notice that a person in Washington State was fraudulently attempting to use her Social Security Number.

19. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect herself from data breaches, and reviewing her financial accounts for fraud or suspicious activity. She now plans to spend several hours a month checking account statements for irregularities.

20. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her PII, which she expected AT&T to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. Plaintiff Jeryl Luciani

21. Plaintiff Jeryl Luciani is a citizen of and is domiciled in the state of Florida.

22. Plaintiff is a current customer of AT&T.

23. Plaintiff provided confidential and sensitive PII to AT&T, as requested and required by AT&T for the provision of its services. AT&T obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

24. Plaintiff would not have entrusted her PII to AT&T had she known that AT&T failed to maintain adequate data security.

25. On or about March 30, 2024, Plaintiff received the following email from AT&T:

Keeping Your Account Secure

Dear Jeryl,

We take cybersecurity very seriously and privacy is a fundamental commitment at AT&T.

We have discovered that your AT&T account passcode has been compromised, therefore we have proactively reset your passcode.

Our internal teams are working with external cybersecurity experts to analyze the situation. It appears the data is from more than 4 years ago and does not contain personal financial information or call history.

What information was involved?
The information varied by customer and account, but may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode.

If your sensitive personal information was compromised, we will provide complimentary identity theft and credit monitoring services.

What is AT&T doing?
We've taken precautionary measures and reset your passcode, which is an extra layer of protection for your account. When you sign in to your online account or call customer care, we'll provide details to help you personalize your passcode.

What can you do?
In addition to resetting your AT&T passcode, we encourage customers to remain vigilant by monitoring account activity and credit reports. You can set up free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. You can also request and review your free credit report at any time via Freecreditreport.com.

More Information
Visit www.att.com/accountsafety for more information and updates.

We apologize this has happened and are committed to keeping your account secure.

AT&T

26. Subsequently, on or about April 11, 2024, Plaintiff received this follow-on notification from AT&T that his information was compromised:

AT&T Security Update

Dear Jeryl,

We recently contacted you regarding the security of your data. After a thorough assessment, AT&T has determined that some of your personal information was compromised. To the best of our knowledge, the compromised data does **not** include personal financial information or call history.

What is AT&T doing to help?
AT&T takes these issues very seriously. To protect your account, we have proactively reset your account passcode. You can personalize your passcode online via myAT&T.

We are also offering you one year of complimentary credit monitoring, identity theft detection and resolution services, provided by Experian's® IdentityWorks℠. To get started with IdentityWorks℠, please follow the instructions below and **enroll by August 30, 2024.**

Where can you get more information?
Visit att.com/accountsafety for more details.

We apologize this has happened. You are a valued customer and we are committed to keeping your information secure.

AT&T

27. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect herself from data breaches, and reviewing her financial accounts for fraud or suspicious activity. She now plans to spend several hours a month checking account statements for irregularities.

28. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her PII, which she expected AT&T to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her PII. As a result

of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

C. Plaintiff Michael Crain

29. Plaintiff Michael Crain is a citizen of and is domiciled in the state of Texas.

30. Plaintiff is a present customer of AT&T for cellular telephone services.

31. Plaintiff provided confidential and sensitive PII to AT&T, as requested and required by AT&T for the provision of its services. AT&T obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

32. Plaintiff would not have entrusted his PII to AT&T had he known that AT&T failed to maintain adequate data security.

33. On or about March 30, 2024, Plaintiff received the following email from AT&T:

Keeping Your Account Secure

Dear Michael,

We take cybersecurity very seriously and privacy is a fundamental commitment at AT&T.

We have discovered that your AT&T account passcode has been compromised, therefore we have proactively reset your passcode.

Our internal teams are working with external cybersecurity experts to analyze the situation. It appears the data is from more than 4 years ago and does not contain personal financial information or call history.

What information was involved?
The information varied by customer and account, but may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode.

What is AT&T doing?
We've taken precautionary measures and reset your passcode, which is an extra layer of protection for your account. When you sign in to your online account or call customer care, we'll provide details to help you personalize your passcode. If your sensitive personal information was compromised, we will provide complimentary identity theft and credit monitoring services.

What can you do?
In addition to resetting your AT&T passcode, we encourage customers to remain vigilant by monitoring account activity and credit reports. You can set up free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. You can also request and review your free credit report at any time via Freecreditreport.com.

More Information
Visit www.att.com/accountsafety for more information and updates.

We apologize this has happened and are committed to keeping your account secure.

AT&T

34. Subsequently, on or about April 11, 2024, plaintiff received this follow-on notification from AT&T that his information was compromised:

AT&T Security Update

Dear Michael,

We recently contacted you regarding the security of your data. After a thorough assessment, AT&T has determined that some of your personal information was compromised. To the best of our knowledge, the compromised data does **not** include personal financial information or call history.

What is AT&T doing to help?
AT&T takes these issues very seriously. To protect your account, we have proactively reset your account passcode. You can personalize your passcode online via myAT&T.

We are also offering you one year of complimentary credit monitoring, identity theft detection and resolution services, provided by Experian's® IdentityWorks℠. To get started with IdentityWorks℠, please follow the instructions below and **enroll by August 30, 2024.**

Where can you get more information?
Visit att.com/accountsafety for more details.

We apologize this has happened. You are a valued customer and we are committed to keeping your information secure.

AT&T

35. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself

from data breaches, and reviewing his financial accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

36. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his PII, which he expected AT&T to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

D. Defendant

37. Defendant AT&T, Inc. is a Delaware corporation with its principal place of business in Dallas, Texas. It provides Internet, landline, television and wireless voice and data services throughout the United States, including for approximately 241 million cellular network subscribers.[6]

38. In the course of its business, AT&T collect names, phone numbers, Social Security numbers, physical addresses, driver's license information, and other information from its customers and prospective customers.

IV. FACTUAL BACKGROUND

A. AT&T Failed to Adequately Protect Customer Data, Resulting in the Data Breach

1. When first presented with evidence of the Data Breach, AT&T denied that it occurred.

39. Customer PII from the Data Breach first appeared for sale nearly three years ago. In August 2021, ShinyHunters, a known criminal hacking group, posted for sale "AT&T Database +70M (SSN/DOB)" on a hacker forum and marketplace.[7] ShinyHunters stated they would sell the database immediately for $1 million.

[6] AT&T Q4 2023 8K Earnings Report, accessible at: https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2023/4q-2023/ATT_4Q_2023_8_K_Earnings_8_01.pdf (last visited April 4, 2024).

[7] Waqas, AT&T breach? ShinyHunters selling AT&T database with 70 million SSN, HACKREAD (Aug. 20, 2021), https://www.hackread.com/att-breach-shinyhunters-database-selling-70-million-ssn/.

40. Hackread, one of the technology sites that reported the auctioning of the data online noted:[8]

> Hackread.com has seen the sample records shared by ShinyHunters on the forum and a quick review of it reveals that these records include the following customers' details:
>
> - Full names
> - Addresses
> - Zipcodes
> - Date of birth
> - Email addresses
> - Social security numbers (SSN)

41. AT&T learned of the auction of this data, but in response claimed that the data did not come from its servers.[9]

2. Three years later, AT&T finally admits the Data Breach occurred.

42. On March 17, 2024, MajorNelson provided free of charge on a hacking forum a database containing over 73 million records that appeared to contain AT&T customer information. Analysis showed that this database was the same set of information that had been offered for sale by ShinyHunters three years earlier.[10]

43. But this time, when faced with the same set of customer information that included AT&T account-specific information, the massive Data breach was no longer deniable by AT&T. AT&T admitted that its systems were compromised:

> AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set,

[8] *Id.*

[9] Lawrence Abrams, AT&T denies data breach after hacker auctions 70 million user database, BLEEPINGCOMPUTER (Aug. 20, 2021, 9:43 AM), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after- hacker-auctions-70-million-user-database/.

[10] Lawrence Abrams, AT&T says leaked data of 70 million people is not from its systems, BLEEPINGCOMPUTER (Mar. 17, 2024, 7:24 PM), https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70- million-people-is-not-from-its-systems/.

> which includes personal information such as social security numbers, the source of the data is still being assessed.
>
> AT&T has launched a robust investigation supported by internal and external cybersecurity experts. Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.
>
> Currently, AT&T does not have evidence of unauthorized access to its systems resulting in exfiltration of the data set. The company is communicating proactively with those impacted and will be offering credit monitoring at our expense where applicable. We encourage current and former customers with questions to visit www.att.com/accountsafety for more information.
>
> As of today, this incident has not had a material impact on AT&T's operations.[11]

44. After falsely denying its systems were breached in August 2021, AT&T appears to have done nothing at all to protect its 73 million current and former customers from the effects of its negligence for the following nearly three years. AT&T now claims to have "launched a robust investigation supported by internal and external cybersecurity experts," something it should have done in 2021 to have any hope of actually mitigating the extensive harm its false denial has—and not doubt will—cause for years to come.

45. AT&T was familiar with its obligations—created by contract, industry standards, common law, and representations to its customers—to protect customer information. Plaintiffs and Class Members provided their Private Information to AT&T with the reasonable expectation that AT&T would comply with its obligations to keep such information confidential and secure.

46. AT&T failed to comply with these obligations, resulting in the Data Breach. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records.

B. The Data Breach Puts Consumers at Increased Risk of Fraud and Identity Theft

47. An identity thief uses victims' PII, such as name, address, and other sensitive and confidential information, without permission, to commit fraud or other crimes that range from

[11] *Id.*

immigration fraud, obtaining a driver's license or identification card, obtaining government benefits, and filing fraudulent tax returns to obtain tax refunds.

48. Identity thieves can use a victim's PII to open new financial accounts, incur charges in the victim's name, take out loans in the victim's name, and incur charges on existing accounts of the victim. Plaintiffs' finances are now at risk due to the Data Breach.

49. Identity theft is the most common consequence of a data breach—it occurs to 65% of data breach victims.[12] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[13]

50. Plaintiffs are now in the position of having to take steps to mitigate the damages caused by the Data Breach. Once use of compromised non-financial PII is detected, the emotional and economic consequences to the victims are significant. Studies done by the ID Theft Resource Center, a non-profit organization, found that victims of identity theft had marked increased fear for personal financial security. The report attributes this to more people having been victims before, contributing to greater awareness and understanding that they may suffer long term consequences from this type of crime.[14]

51. AT&T failed to protect and safeguard Plaintiffs' and Class Members' private information, in fact failing to adhere to even its most basic obligations. As a result, Plaintiffs and Class Members have suffered or will suffer actual injury, including loss of privacy, costs, and loss of time.

V. CLASS ACTION ALLEGATIONS

52. Plaintiffs bring this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the "Class"), defined as:

> All natural persons in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

---

[12] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last visited Feb. 1, 2023).

[13] *Id.*

[14] Identity Theft: The Aftermath 2013, Identity Theft Resource Center, https://idtheftinfo.org/latest-news/72 (last visited Feb. 1, 2023).

53. In addition, the State Subclasses are defined as follows:

> **Tennessee Subclass:** All natural persons in the State of Tennessee whose Personally Identifiable Information was compromised as a result of the Data Breach.
>
> **Florida Subclass:** All natural persons in the State of Florida whose Personally Identifiable Information was compromised as a result of the Data Breach.
>
> **Texas Subclass:** All natural persons in the State of Texas whose Personally Identifiable Information was compromised as a result of the Data Breach.

54. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of Defendant. Nevertheless, the Class encompasses at least 73 million individuals dispersed throughout the United States. The number of Class Members is so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendant.

55. **Commonality and Predominance:** This action involves common questions of law and fact which predominate over any question solely affecting individual Class Members. These common questions include:

a) whether Defendant engaged in the conduct alleged herein;

b) whether Defendant had a legal duty to use reasonable security measures to protect Plaintiffs' and Class Members' PII;

c) whether Defendant timely, accurately, and adequately informed Plaintiffs and Class Members that their PII had been compromised;

d) whether Defendant breached their legal duty by failing to protect the PII of Plaintiffs and Class Members;

e) whether Defendant acted reasonably in securing the PII of Plaintiffs and Class Members;

f) whether Plaintiffs and Class Members are entitled to injunctive relief;

g) and whether Plaintiffs and Class Members are entitled to damages and equitable relief.

56. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendant's substantially uniform

misconduct, as described above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other members of the Class that they represent, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and Class Members arise from the same operative facts and are based on the same legal theories.

57. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiffs and their counsel.

58. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be virtually impossible for the Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not: individualized litigation creates a potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

VI. CAUSES OF ACTION

A. Claims Brought on Behalf of the Nationwide Class

COUNT ONE
NEGLIGENCE

59. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

60. AT&T owed a duty to Plaintiffs and Class Members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care

in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing AT&T's networks, systems, protocols, policies, procedures, and practices to ensure that Plaintiffs' and Class Members' information was adequately secured from unauthorized access.

61. AT&T's Privacy Notice acknowledged AT&T's duty to adequately protect Plaintiffs' and Class Members' PII.

62. AT&T owed a duty to Plaintiffs and Class Members to implement administrative, physical, and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Class Members' PII.

63. AT&T also had a duty to only maintain PII that was needed to serve customer needs.

64. AT&T owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

65. AT&T also had independent duties under Plaintiffs' and Class Members' state laws that required AT&T to reasonably safeguard Plaintiffs' and Class Members' PII, and promptly notify them about the Data Breach.

66. AT&T had a special relationship with Plaintiffs and Class Members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiffs' and Class Members' willingness to entrust AT&T with their PII was predicated on the understanding that AT&T would take adequate security precautions. Moreover, AT&T was capable of protecting its networks and systems, and the PII it stored on them, from unauthorized access.

67. AT&T breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiffs' and Class Members' PII, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

68. But for AT&T's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

69. Plaintiffs and Class Members were foreseeable victims of AT&T's inadequate data security practices. AT&T knew or should have known that a breach of its data security systems would cause damage to Plaintiffs and Class Members.

70. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII would result in unauthorized access to AT&T's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' PII.

71. As a result of AT&T's negligent failure to prevent the Data Breach, Plaintiffs and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

72. The harm to Plaintiffs and Class Members was a proximate, reasonably foreseeable result of AT&T's breaches of its aforementioned duties.

73. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

74. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

75. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, AT&T had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

76. In addition, under state data security statutes, AT&T had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

77. AT&T breached its duties to Plaintiffs and Class Members, under the Federal Trade Commission Act, 15 U.S.C. § 45, ("FTCA") and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

78. Plaintiffs and Class Members were foreseeable victims of AT&T's violations of the FTCA and state data security statutes. AT&T knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

79. AT&T's failure to comply with the applicable laws and regulations constitutes negligence *per se.*

80. But for AT&T's violation of the applicable laws and regulations, Plaintiffs,' and Class Members' PII would not have been accessed by unauthorized parties.

81. As a result of AT&T's failure to comply with applicable laws and regulations, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

82. The harm to Plaintiffs and the Class Members was a proximate, reasonably foreseeable result of AT&T's breaches of the applicable laws and regulations.

83. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT THREE
GROSS NEGLIGENCE

84. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

85. Plaintiffs and Class Members entrusted AT&T with highly sensitive and inherently personal private data subject to confidentiality laws.

86. In requiring, obtaining, and storing Plaintiffs' and Class Members' PII, AT&T owed a duty of reasonable care in safeguarding the PII.

87. AT&T's networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII were secured from unauthorized access.

88. AT&T's networks, systems, protocols, policies, procedures, and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class Members' private data and the known vulnerabilities of AT&T's systems.

89. AT&T did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

90. Upon learning of the Data Breach, AT&T should have immediately disclosed the Data Breach to Plaintiffs and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions and all other third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class Members as a result of the Data Breach.

91. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class Members' PII were secured from unauthorized access, AT&T ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

92. AT&T's behavior establishes facts evidencing a reckless disregard for Plaintiffs' and Class Members' rights.

93. AT&T, therefore, was grossly negligent.

94. AT&T's negligence also constitutes negligence per se.

95. Negligence is directly linked to injuries.

96. As a result of AT&T's reckless disregard for Plaintiffs' and Class Members' rights by failing to secure their PII, despite knowing its networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

97. The harm to Plaintiffs and the Class Members was a proximate, reasonably foreseeable result of AT&T's breaches of the applicable laws and regulations.

98. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT FOUR
BREACH OF EXPRESS CONTRACTS

99. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

100. Plaintiffs and members of the Class, additionally and alternatively, allege that they entered into valid and enforceable express contracts with AT&T.

101. Under these express contracts, AT&T promised and was obligated to: (a) provide services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PII. In exchange, Plaintiffs and members of the Class agreed to pay money for these services.

102. Both the provision of services, as well as the protection of Plaintiffs' and Class Members' PII, were material aspects of these contracts.

103. AT&T's express representations, including, but not limited to, express representations found in AT&T's Privacy Notice, formed an express contract requiring AT&T to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

104. Alternatively, the express contracts included implied terms requiring AT&T to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII, including in accordance with federal, state, and local laws, and industry standards.

105. Consumers value their privacy, the privacy of their dependents, and the ability to keep their PII associated with obtaining services private. To customers such as Plaintiffs and Class Members, services that do not adhere to industry-standard data security protocols to protect PII are fundamentally less useful and less valuable than services that adhere to industry-standard data security. Plaintiffs and Class Members would not have entered into these contracts with AT&T without an understanding that their PII would be safeguarded and protected.

106. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PII to AT&T and paid for the provided services in exchange for, amongst other things, protection of their PII.

107. AT&T materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Specifically, AT&T did not comply with federal, state, and local laws, or industry standards, or otherwise protect Plaintiffs' and the Class Members' PII, as set forth above. Further, on information and belief, AT&T has not yet provided Data Breach notifications to some affected Class Members who may already be victims of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud associated with PII that they provided to AT&T. These Class Members are as yet unaware of the potential source for the compromise of their PII.

108. The Data Breach was a reasonably foreseeable consequence of AT&T's actions in breach of these contracts.

109. As a result of AT&T's failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

110. Had AT&T disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs, nor Class Members, nor any reasonable person would have purchased services from AT&T.

111. As a result of AT&T's breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain in imminent risk of suffering additional damages in the future.

112. As a result of AT&T's breach, Plaintiffs and the Class Members have suffered actual damages resulting from their attempt to mitigate the effects of the breach of contract and subsequent Data Breach, including but not limited to, taking steps to protect themselves from the loss of their PII.

113. Accordingly, Plaintiffs and the other members of the Class have been injured as a result of AT&T's breach of contract and are entitled to damages and/or restitution in an amount to be determined at trial.

COUNT FIVE
BREACH OF IMPLIED CONTRACTS

114. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

115. Plaintiffs and Class Members were required to provide their PII to obtain services from AT&T. Plaintiffs and Class Members entrusted their PII to AT&T in order to obtain services from them.

116. By providing their PII, and upon AT&T's acceptance of such information, Plaintiffs and Class Members on one hand, and AT&T on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express

contracts concerning the services provided, whereby AT&T was obligated to take reasonable steps to secure and safeguard that information.

117. AT&T had an implied duty of good faith to ensure that the PII of Plaintiffs and Class Members in its possession was only used in accordance with their contractual obligations.

118. AT&T was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and state laws and regulations for the security of this information, and AT&T expressly assented to these terms in its Privacy Notice as alleged above.

119. Under these implied contracts for data security, AT&T was further obligated to provide Plaintiffs and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

120. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to AT&T, including paying for the services provided by AT&T and/or providing the PII required by AT&T.

121. AT&T breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, resulting in the Data Breach. AT&T unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members.

122. Further, on information and belief, AT&T has not yet provided Data Breach notifications to some affected Class Members who may already be victims of identity fraud or theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the PII that they provided to AT&T. These Class Members are unaware of the potential source for the compromise of their PII.

123. The Data Breach was a reasonably foreseeable consequence of AT&T's actions in breach of these contracts.

124. As a result of AT&T's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value as compared to the secure services they paid for. Plaintiffs and Class Members, therefore, were

damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

125. Neither Plaintiffs, nor Class Members, nor any reasonable person would have provided their PII to AT&T had AT&T disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

126. As a result of AT&T's breach, Plaintiffs and Class Members have suffered actual damages resulting from theft of their PII, as well as the loss of control of their PII, and remain in imminent risk of suffering additional damages in the future.

127. As a result of AT&T's breach, Plaintiffs and the Class Members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII. As a result, Plaintiffs and the Class Members have suffered actual identity theft and the ability to control their PII.

128. Accordingly, Plaintiffs and Class Members have been injured as a result of AT&T's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT SIX
BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING

129. Plaintiffs reallege and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

130. Plaintiffs and Class Members entered into and/or were the beneficiaries of contracts with Defendant, as alleged above.

131. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendant would act fairly, reasonably, and in good faith in carrying

out their contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and federal and state laws and regulations for the security of this information.

132. Special relationships exist between Defendant and Plaintiffs and Class Members. Defendant entered into special relationships with Plaintiffs and Class Members, who entrusted their confidential PII to Defendant and paid for services with Defendant.

133. Defendant promised and was obligated to protect the confidentiality of Plaintiffs' and Class Members' PII from disclosure to unauthorized third parties. Defendant breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, which resulted in the Data Breach. Defendant unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the PII of Plaintiffs and the Class in Defendant's possession.

134. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant, including paying Defendant for services, and providing it the confidential PII required by the contracts.

135. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members did not receive the full benefit of their bargain—services with reasonable data privacy—and instead received services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members have suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

136. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from the theft of their PII and remain at imminent risk of suffering additional damages in the future.

137. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII.

138. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class Members suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendant from its conduct. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law.

COUNT SEVEN
UNJUST ENRICHMENT
(ALTERNATIVE TO BREACH OF CONTRACT CLAIM)

139. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

140. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for services received.

141. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by Plaintiffs and Class Members.

142. The money that Plaintiffs and Class Members paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data management and security. Defendant failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

143. As a result of Defendant's failure to implement security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

144. Under principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members because Defendant failed to implement the data management and security measures that are mandated by industry standards and that Plaintiffs and Class Members paid for.

145. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by Defendant. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendant traceable to Plaintiffs and the Class.

COUNT EIGHT
DECLARATORY JUDGMENT

146. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

147. Plaintiffs and the Class have stated claims against Defendant based on negligence, negligence per se, gross negligence and negligent misrepresentation, and violations of various state and federal statutes.

148. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII of Plaintiffs and the Class, as evidenced by the Data Breach.

149. As a result of the Data Breach, Defendant's system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII of Plaintiffs and the Class going forward.

150. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Class. Defendant maintains that its security measures were—and still are—reasonably adequate and denies that it previously had or has any obligation to implement better safeguards to protect the PII of Plaintiffs and the Class.

151. Plaintiffs seek a declaration that Defendant must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that Defendant's

existing security measures do not comply with their obligations, and that Defendant must implement and maintain reasonable security measures on behalf of Plaintiffs and the Class to comply with their data security obligations.

B. Claims Brought on Behalf of the Florida Subclass

COUNT NINE
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. §§ 501.201, et seq.

152. Plaintiff Luciani, individually and on behalf of the Florida Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually and on behalf of the Florida Subclass under the laws of Florida.

153. Plaintiff Luciani and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

154. AT&T advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

155. AT&T engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Florida Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. Ann. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. Ann. § 501.171(2);

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Florida Subclass Members' PII; and

g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. Ann. § 501.171(2).

156. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

157. Had AT&T disclosed to Plaintiff and Florida Subclass Members that its data systems were not secure and thus vulnerable to attack; AT&T would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Florida Subclass. AT&T accepted the responsibility of protecting the data, while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Florida Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

158. As a direct and proximate result of AT&T's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, as described herein, including but not limited to one or more of the following: ongoing,

imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; (iv) illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of PII; lost value of access to PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefits of bargains as well as overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

159. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

C. Claims Brought on Behalf of the Tennessee Subclass

COUNT TEN
TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT,
Tenn. Code Ann. §§ 47-18-2107, et seq.

160. Plaintiff Garner, individually and on behalf of the Tennessee Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually and on behalf of the Tennessee Subclass under the laws of Tennessee.

161. AT&T is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

162. Plaintiff's and Tennessee Subclass Members' PII (e.g., Social Security numbers) include PII as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

163. AT&T is required to accurately notify Plaintiff and Tennessee Subclass Members following discovery or notification of a breach of its data security system in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

164. Because AT&T discovered a breach of its security system in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, AT&T had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

165. By failing to disclose the Data Breach in a timely and accurate manner, AT&T violated Tenn. Code Ann. § 47-18-2107(b).

166. As a direct and proximate result of AT&T's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass Members suffered damages, as described above.

167. Plaintiff and Tennessee Subclass Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

COUNT ELEVEN
TENNESSEE CONSUMER PROTECTION ACT, Tenn. Code Ann. §§ 47-18-101, et seq.

168. Plaintiff Garner, individually and on behalf of the Tennessee Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually and on behalf of the Tennessee Subclass under the laws of Tennessee.

169. AT&T is a "person," as defined by Tenn. Code § 47-18-103(13).

170. Plaintiff and Tennessee Subclass Members are "consumers," as meant by Tenn. Code § 47-18-103(2).

171. AT&T advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

172. AT&T advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And AT&T's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

173. AT&T's unfair and deceptive acts and practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass members' PII; and

g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

174. AT&T intended to mislead Plaintiff and Tennessee Subclass Members and induce them to rely on its misrepresentations and omissions.

175. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

176. Had AT&T disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. AT&T accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

177. AT&T had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Subclass, and AT&T because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in AT&T. AT&T's duty to disclose also arose from its:

a) Possession of exclusive knowledge regarding the security of the data in its systems;

b) Active concealment of the state of its security; and/or

c) Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Tennessee Subclass that contradicted these representations.

178. AT&T's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

179. The injury to consumers was and is substantial because it was non-trivial and non-speculative and involved a monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only

because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

180. Consumers could not have reasonably avoided injury because AT&T's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, AT&T created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

181. AT&T's inadequate data security had no countervailing benefit to consumers or to competition.

182. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), AT&T violated the following provisions of Tenn. Code § 47-18-104(b):

a) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b) Representing that goods or services are of a particular standard, quality, or grade, if they are of another;

c) Advertising goods or services with intent not to sell them as advertised; and

d) Representing that a consumer transaction confers or involves rights, remedies, or obligations that it does not have or involve.

183. AT&T acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

184. As a direct and proximate result of AT&T's unfair and deceptive acts or practices, Plaintiff and Tennessee Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related

to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

185. AT&T's violations present a continuing risk to Plaintiff and Tennessee Subclass Members as well as to the general public.

186. Plaintiff and Tennessee Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

D. Claims Brought on Behalf of the Texas Subclass

COUNT TWELVE
DECEPTIVE TRADE PRACTICES—
CONSUMER PROTECTION ACT,
Texas Bus. & Com. Code §§ 17.41, et seq.

187. Plaintiff Crain, individually and on behalf of the Texas Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually and on behalf of the Texas Subclass under the laws of Texas.

188. AT&T is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

189. Plaintiff and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

190. AT&T advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

191. AT&T engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a) Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b) Representing that goods or services are of a particular standard, quality, or grade, if they are of another;

c) Advertising goods or services with intent not to sell them as advertised; and

d) Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

192. AT&T's false, misleading, and deceptive acts and practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass members' PII; and

g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and

Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

193. AT&T intended to mislead Plaintiff and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

194. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' PII.

195. Had AT&T disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. AT&T was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. AT&T accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they could not have discovered.

196. AT&T had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Texas Subclass, and AT&T because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in AT&T. AT&T's duty to disclose also arose from its:

a) Possession of exclusive knowledge regarding the security of the data in its systems;

b) Active concealment of the state of its security; and/or

c) Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Texas Subclass that contradicted these representations.

197. AT&T engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). AT&T engaged in acts or practices which, to

consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

198. Consumers, including Plaintiff and Texas Subclass Members, lacked knowledge about deficiencies in AT&T's data security because this information was known exclusively by AT&T. Consumers also lacked the ability, experience, or capacity to secure the PII in AT&T's possession or to fully protect their interests with regard to their data. Plaintiff and Texas Subclass Members lack expertise in information security matters and do not have access to AT&T's systems in order to evaluate its security controls. AT&T took advantage of its special skill and access to PII to hide its inability to protect the security and confidentiality of Plaintiff and Texas Subclass Members' PII.

199. AT&T intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from AT&T's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The AT&T data breach, which resulted from AT&T's unconscionable business acts and practices, exposed Plaintiff and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

200. AT&T acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass Members' rights. AT&T's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

201. As a direct and proximate result of AT&T's unconscionable and deceptive acts or practices, Plaintiff and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of

value of their PII; overpayment for AT&T's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach. AT&T's unconscionable and deceptive acts or practices were a producing cause of Plaintiff's and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non- economic damages, including their mental anguish.

202. AT&T's violations present a continuing risk to Plaintiff and Texas Subclass Members as well as to the general public.

203. Plaintiff and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

VII. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and on behalf of the proposed Class and Subclasses, request that the Court:

a. Certify this case as a class action, appoint Plaintiffs as class representative, and appoint Plaintiffs' Counsel as Class Counsel for Plaintiffs to represent the Class;

b. Find that AT&T breached its duty to safeguard and protect the PII of Plaintiffs and Class Members that was compromised in the Data Breach;

c. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution, and disgorgement;

d. Award equitable, injunctive, and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated April 19, 2024

Respectfully submitted,

HILLIARD LAW

By: *Robert C. Hilliard*
Robert C. Hilliard
State Bar No.: 09677700
Federal Bar No.: 5912
719 S. Shoreline Blvd.
Corpus Christi, Texas 78401
Telephone No.: (361) 882-1612
Facsimile No.: (361) 882-3015

And

COTCHETT PITRE & MCCARTHY LLP

Thomas E. Loeser (*Pro hac vice to be filed*)
Karin B. Swope
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577
tloeser@cpmlegal.com.com
kswope@cpmlegal.com

Andrew F. Kirtley
Gia Jung
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: (650) 697-6000
Fax: (650) 697-0577
akirtley@cpmlegal.com.com
Gjung@cpmlegal.com

Attorneys for Plaintiffs and the proposed Class