FILED
TARRANT COUNTY
3/17/2025 5:29 PM
THOMAS A. WILDER
DISTRICT CLERK

**CAUSE NO. _____**

| | |
|---|---|
| **ALEX LAWRENCE and AMANDA LAWRENCE *ET AL.***, individually and on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>**WHITLEY PENN LLP,**<br><br>Defendant. | **IN THE DISTRICT COURT OF**<br><br>**TARRANT COUNTY, TEXAS**<br><br>**_____ JUDICIAL DISTRICT**<br><br>**JURY TRIAL DEMANDED** |

## PLAINTIFFS' ORIGINAL PETITION

Plaintiffs Alex Lawrence, Amanda Lawrence, Marcus Nordstrom, Alisha Patel, and Jeremy Raphael, individually and on behalf of all others similarly situated, bring this petition against Whitley Penn, LLP (Whitley Penn" or "Defendant"). The following allegations are based on Plaintiffs' knowledge, investigations of counsel, facts of public record, and information and belief.

## DISCOVERY CONTROL PLAN

1. Any discovery is intended to be conducted under Level 2 pursuant to Tex. R. Civ. P. Rule 190.3.

## CLAIM FOR RELIEF

2. Pursuant to Tex. R. Civ. P. 47(c), Plaintiffs seek monetary relief over $250,000 but not more than $1,000,000 in addition to non-monetary relief.

## NATURE OF THE ACTION

3. On January 30, 2024, Whitley Penn, a full-service accounting and advisory firm, disclosed that in late October 2023, it experienced a massive data breach, (the "Data Breach" or "Breach"), resulting in the disclosure and theft of over 700 individuals' highly sensitive non-public

information used to prepare tax returns, including first and last names, addresses, birth dates, driver's license numbers, passport numbers, Social Security numbers, K-1 visa information, taxpayer identification numbers, banking account information, PIN numbers, and other financial information. Plaintiffs' information was stolen in the Breach.

4. Taking reasonable, standard precautions against cybercrime and data breaches is a fundamental part of doing business in the modern age—especially for businesses that profit from analyzing and processing personally identifiable information[1] ("PII") such as the information at issue in this lawsuit. By collecting, maintaining, and profiting from Plaintiffs' and the Class Members' PII, Whitley Penn was required by law to exercise reasonable care and comply with industry and statutory requirements to protect that information—and they failed to do so.

5. Instead, Defendant's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of their negligence. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard its customers' PII and by failing to take available and necessary steps to prevent unauthorized disclosure of that data.

6. The highly sensitive information exfiltrated in the Data Breach includes, but is not limited to, full names, dates of birth, social security numbers, bank account information, PIN numbers, passport numbers, K-1 visa information, taxpayer identification numbers, driver's license numbers, and "certain financial information."[2]

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Ex. 1 – Data Breach Notice Letter

7. Even though it was Defendant's dereliction of duty that led to the Data Breach, it is Plaintiffs and the other victims of the Data Breach, that will bear the burden of Defendant's negligence for years to come.

8. The exponential cost to Plaintiffs and the Class Members resulting from the Data Breach cannot be overstated. Criminals can use victims' names, birth dates, social security numbers, and addresses to open new financial accounts, incur charges in credit, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it.[3] Any one of these instances of identity theft can have devastating consequences for the victim—causing years of often irreversible damage to their credit scores, financial stability, and personal security.

9. Plaintiffs and the Classes are at imminent, certain risk for identity theft because of the nature of the PII exposed.

10. This risk has been maximized by the fact that Defendant waited three months to notify Plaintiffs and Class Members after learning of the Breach, preventing Plaintiffs from taking precautionary measures to secure their data.

11. This delay also contravenes their general duty to their customers to notify their customers of their deficient security measures as well as specific promises that Whitley Penn makes to its customers that it will not "disclose any non-public personal information of current

[3] *See, e.g.*, *Report to Congressional Requesters*, United States Government Accountability Office (June 2007), http://www.gao.gov/assets/270/262899.pdf; Melanie Lockert, *How do hackers use your information for identity theft?*, CreditKarma (Oct. 1, 2021), https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information; Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2020), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it; Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LifeLock by Norton (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft.

and former clients" and that it will "only disclose information to unrelated third parties under a contractual agreement" because Plaintiffs and the class did not consent to their information being disclosed to cybercriminals.

12. Waiting three months to notify Defendant's clients also violates the laws of several jurisdictions and is unreasonable.

13. Adding insult to injury, there has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its security practices sufficient to avoid a similar breach of their network in the future. Indeed, Defendant has disclosed little to no information regarding who illegally accessed Plaintiffs and Class Members' information, why that person or persons were able to access such information, and what steps Defendant has taken since.

14. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) lost value of PII, a form of property that Defendant obtained from Plaintiffs and Class members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their PII; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain risk that unauthorized persons will access and abuse Plaintiffs and Class Members' highly sensitive PII that is available on the dark web; (v) the continued and certain increased risk that the PII that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the PII; (vi) theft of their PII and the resulting loss of privacy rights in that information; (vii) credit freezes and unfreezes; (viii) decreased credit scores; (ix) lost work time; (x) anxiety, annoyance, and nuisance;

and (xi) disgorgement damages associated with Defendant's maintenance and use of Plaintiffs' data for its benefit and profit.

15. As a direct and proximate result of the Data Breach and Defendant's failure to protect Plaintiffs' and the Class Members' unencrypted PII, Plaintiffs and the Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, social engineering, and other misuses of their PII, as well as an increased risk to their personal safety; ongoing monetary loss and economic harm, including loss of value of their PII; loss of value of privacy and confidentiality of the stolen PII; illegal sales of the compromised PII; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries. Plaintiffs and Class Members have a continuing interest in ensuring that their PII is and remains safe, and they should be entitled to injunctive and other equitable relief.

16. Finally, malicious actors will often wait months, or even years, to use stolen PII to lower chances of detection by the victim or temporary credit monitoring assistance. This means that Plaintiffs or the Class Members could be victims of multiple instances of identity theft as a result of this single Data Breach. While Plaintiffs and the Class Members are already at imminent risk for identity theft, such risk will continue, possibly indefinitely, as a direct and foreseeable result of Defendant's negligence.

17. Through this lawsuit, Plaintiffs seek to hold Whitley Penn responsible for the injuries it inflicted on Plaintiffs and over 700 similarly situated persons due to its impermissibly inadequate data security measures.

## PARTIES

### Defendant Whitley Penn LLP

18. Defendant Whitley Penn is a full-service accounting and advisory firm based in Fort Worth, Texas. Defendant is a limited liability partnership formed and existing under the laws of Texas with its headquarters and principal place of business at 640 Taylor St., Suite 2200, Fort Worth, TX 76102.

### Plaintiff Alex Lawrence

19. Plaintiff Alex Lawrence is a resident and citizen of Falls Church, Virginia, where he intends to remain.

20. Plaintiff Alex Lawrence's previous employer entrusted his PII to Whitley Penn as a condition to receiving certain tax, payroll, and/or accounting services.

21. Plaintiff Alex Lawrence received a Notice Letter from Whitley Penn in or around February 2024 concerning the Data Breach and informing him that his PII was compromised in the Data Breach.

22. Plaintiff Alex Lawrence has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit.

23. Plaintiff Alex Lawrence is very careful about sharing sensitive information. He stores any documents concerning sensitive information in a safe and secure location and has never knowingly transmitted unencrypted sensitive information over the Internet or any other unsecured source.

24. Plaintiff Alex Lawrence had the reasonable expectation and understanding that Whitley Penn would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of

any data security incidents. Plaintiff Alex Lawrence would not have entrusted his PII to Whitley Penn had he known that Whitley Penn would not have taken reasonable steps to safeguard his information.

25. As a direct and proximate result of the Data Breach, Plaintiff Alex Lawrence has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud and regularly and closely pulling his credit report.

26. Plaintiff Alex Lawrence has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

27. As a result of the Data Breach, Plaintiff Alex Lawrence anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He faces a present and continuing risk of fraud and identify theft for his lifetime.

**Plaintiff Amanda Lawrence**

28. Plaintiff Amanda Lawrence is a resident and citizen of Falls Church, Virginia, where she intends to remain.

29. Plaintiff Amanda Lawrence's previous employer entrusted her PII to Whitley Penn as a condition to receiving certain tax, payroll, and/or accounting services.

30. Plaintiff Amanda Lawrence received a Notice Letter from Whitley Penn in or around February 2024 concerning the Data Breach and informing her that her PII was compromised in the Data Breach.

31. Plaintiff Amanda Lawrence has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect her credit.

32. Plaintiff Amanda Lawrence is very careful about sharing sensitive information. She stores any documents concerning sensitive information in a safe and secure location and has never knowingly transmitted unencrypted sensitive information over the Internet or any other unsecured source.

33. Plaintiff Amanda Lawrence had the reasonable expectation and understanding that Whitley Penn would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff Amanda Lawrence would not have entrusted her PII to Whitley Penn had she known that Whitley Penn would not have taken reasonable steps to safeguard her information.

34. As a direct and proximate result of the Data Breach, Plaintiff Amanda Lawrence has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud and regularly and closely pulling her credit report.

35. Plaintiff Amanda Lawrence has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

36. As a result of the Data Breach, Plaintiff Amanda Lawrence anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She faces a present and continuing risk of fraud and identify theft for her lifetime.

**Plaintiff Marcus Nordstrom**

37. Plaintiff Marcus Nordstrom is a resident and citizen of Manhattan Beach, California where he intends to remain.

38. Plaintiff Nordstrom's previous employer entrusted his PII to Whitley Penn as a condition to receiving certain tax, payroll and/or accounting services.

39. Plaintiff Nordstrom received a Notice Letter from Whitley Penn in or around February 2024 concerning the Data Breach and informing him that his PII was compromised in the Data Breach.

40. Plaintiff Nordstrom has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit.

41. Plaintiff Nordstrom is very careful about sharing sensitive information. He stores any documents concerning sensitive information in a safe and secure location and has never knowingly transmitted unencrypted sensitive information over the Internet or any other unsecured source.

42. Plaintiff Nordstrom had the reasonable expectation and understanding that Whitley Penn would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff Nordstrom would not have entrusted his PII to Whitley Penn had he known that Whitley Penn would not have taken reasonable steps to safeguard his information.

43. As a direct and proximate result of the Data Breach, Plaintiff Nordstrom has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud, regularly and closely pulling his credit report, and purchasing a software to scrub his personal information from the internet following the Breach.

44. Plaintiff Nordstrom has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

45. As a result of the Data Breach, Plaintiff Nordstrom anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He faces a present and continuing risk of fraud and identify theft for his lifetime.

**Plaintiff Jeremy Raphael**

46. Plaintiff Jeremy Raphael is a resident and citizen of New York, New York where he intends to remain.

47. Plaintiff Raphael's previous employer entrusted his PII to Whitley Penn as a condition to receiving certain tax, payroll and/or accounting services.

48. Plaintiff Raphael received a Notice Letter from Whitley Penn in or around February 2024 concerning the Data Breach and informing him that his PII was compromised in the Data Breach.

49. Plaintiff Raphael has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect his credit.

50. Plaintiff Raphael is very careful about sharing sensitive information. He stores any documents concerning sensitive information in a safe and secure location and has never knowingly transmitted unencrypted sensitive information over the Internet or any other unsecured source.

51. Plaintiff Raphael had the reasonable expectation and understanding that Whitley Penn would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff Raphael would not have entrusted his PII to Whitley Penn had he known that Whitley Penn would not have taken reasonable steps to safeguard his information.

52. As a direct and proximate result of the Data Breach, Plaintiff Raphael has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his accounts for fraud.

53. Plaintiff Raphael has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

54. As a result of the Data Breach, Plaintiff Raphael anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He faces a present and continuing risk of fraud and identify theft for his lifetime.

**Plaintiff Alisha Patel**

55. Plaintiff Alisha Patel is a resident and citizen of Hamlin, Texas, where she intends to remain.

56. Plaintiff Patel's previous employer entrusted her PII to Whitley Penn as a condition to receiving certain tax, payroll and/or accounting services.

57. Plaintiff Patel received a Notice Letter from Whitley Penn in or around February 2024 concerning the Data Breach and informing her that her PII was compromised in the Data Breach.

58. Plaintiff Patel has been experiencing anxiety and stress as a result of the Data Breach and is concerned about how the Data Breach will affect her credit.

59. Plaintiff Patel is very careful about sharing sensitive information. She stores any documents concerning sensitive information in a safe and secure location and has never knowingly transmitted unencrypted sensitive information over the Internet or any other unsecured source.

60. Plaintiff Patel had the reasonable expectation and understanding that Whitley Penn would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff Patel would not have entrusted her PII to Whitley Penn had she known that Whitley Penn would not have taken reasonable steps to safeguard her information.

61. As a direct and proximate result of the Data Breach, Plaintiff Patel has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her accounts for fraud and regularly and closely pulling her credit report.

62. Plaintiff Patel has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

63. As a result of the Data Breach, Plaintiff Patel anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She faces a present and continuing risk of fraud and identify theft for her lifetime.

## JURISDICTION AND VENUE

64. This Court has subject matter jurisdiction over this action because Defendant's negligent conduct occurred in Tarrant County, Texas.

65. This Court has personal jurisdiction over Whitley Penn because it is a resident of the State of Texas.

66. Venue is proper in this County under Tex. Civ. Prac. & Rem. Code § 15.002(a)(1) because a substantial part of the events or omissions giving rise to the claim emanated from activities within this County, and Defendant conducts substantial business in this County.

## FACTUAL ALLEGATIONS

### Whitley Penn Accesses and Stores Its Customers Personally Identifiable Information and Promises to Safeguard the Same

67. Whitley Penn was founded in 1983, employs over 600 people and generates approximately $164.8 million in annual revenue.

68. Whitley Penn is one of the largest accounting firms in the United States and ranks 40 on Accounting Today's 2022 list of the top 100 firms.

69. Whitley Penn provides a wide range of accounting-related services, including tax preparation, employee benefits, estate and gift planning, IRS controversies, and forensic, litigation & valuation services.

70. Defendant Whitley Penn receives its clients' PII as a condition to providing its services.

71. Whitley Penn's website includes a Privacy Policy as of November 1, 2021.[4] The Privacy Policy states:

> Your privacy is very important to us. Public Accounting and Consulting firms are required by law to inform clients of their policies regarding privacy of client information. **CPAs are bound by professional standards of confidentiality that are even more stringent than those required by law**. (emphasis added)

72. Importantly, the Privacy Policy contains a section titled "Parties to Whom We Disclose Information" which reads as follows:

> **We do not disclose any non-public personal information of current and former clients obtained in the course of our practice except as required or permitted by law**. Permitted disclosures include providing information to our employees, and in limited situations, to unrelated third parties who need that information to assist us in providing services to you. In all such situations, we stress the confidential nature of the information being provided. **Whitley Penn LLP will only disclose information to unrelated third parties under a contractual agreement that prohibits them from disclosing or using the information for any purpose other than the specific purpose for which it was disclosed**. (emphasis added)

[4] https://www.whitleypenn.com/privacy-policy/

73. The Privacy Policy touts Whitley Penn's security measures:

> We adhere to strict confidentiality of all client information as required by professional standards and our firm code of conduct. Data protection is achieved through a variety of systems and processes including encrypted laptops, remote access through a secure VPN connection, and the use of a secure portal system to transfer client information. We have implemented and monitored a variety of network security tools, such as firewalls, network intrusion systems with antivirus, and antimalware programs.

74. Given the sensitive nature of the private information Defendant collects as a full-scale accounting and advisory firm, and that Defendant profits from collecting this private information, Defendant further promises in its Privacy Policy that it maintains "physical, electronic, and procedural safeguards that comply with professional standards."

**Whitley Penn Waited Three Months to Notify its Customers of the Data Breach**

75. On January 30, 2024, Whitley Penn disclosed to its impacted customers it experienced a massive data breach by mailing Notice Letters.

76. According to the Notice Letter, the Data Breach occurred sometime before October 31, 2023, when Whitley Penn became aware of the Breach due to "suspicious activity within a certain Whitley Penn email account."[5]

77. While Defendant "immediately" investigated the incident, it waited a stunning three months to notify its impacted customers of the breach.

78. Not only was the disclosure inexcusably late, it was also unconscionably vague and self-serving. Instead of providing detailed information that consumers could use to protect

[5] Interestingly, the Office of the Maine Attorney General's data breach notification states that the breach occurred on September 5, 2023 and it was discovered on October 5, 2023. This discrepancy in information is unacceptable to consumers, and if the dates on the Maine website are accurate, Defendant's delay in notifying impacted customers is even more unacceptable. https://apps.web.maine.gov/online/aeviewer/ME/40/9555bbf5-ed1c-401d-9d7f-abe3397fb833.shtml.

themselves, the Notice Letter merely explained that Defendant's investigation, which concluded on November 21, 2023, determined that the breach was the result of a "malicious cyberattack" without explanation as to what caused the breach, which systems were exposed, and why Defendant chose to wait so long to notify its customers.

79. Further, Defendant provided no information regarding the nature and scope of the attack and whether its vulnerabilities been fixed, which person or person(s) or cybercriminal group were involved with the attack, whether the exposed information is on the dark web, the size of the attack, or what vulnerability in Defendant's system permitted such an attack to occur.

80. A data breach notification submitted to the Office of the Maine Attorney General describes the breach as follows "Lost credentials. User lost control of credentials in an undetermined manner and bad actor used them to access systems."

81. Further, while Whitley Penn notified its impacted customers that it "reviewed its existing policies and procedures and implemented additional administrative and technical safeguards to further secure the information in [its] systems[,]" it provided no detail into what improvements were made.

82. Whitley Penn offered Plaintiffs and Class Members complimentary access to Experian Identity Works for 24 months, demonstrating that they face an imminent, immediate, and continuing increased risk of additional harm from identity theft or identity fraud.

83. Whitley Penn did not offer to take any other steps to help the consumers whose PII it failed to protect.

84. Whitley Penn's failure to provide prompt and adequate notification of the Data Breach injured Plaintiffs and Class Members. Timely and complete notification of a data breach

is essential so consumers can take steps to prevent misuse of the information, mitigate harm that has already occurred, and avoid additional harm.

85. Whitley Penn's inadequate communications have left Plaintiffs and Class Members in the dark regarding the extent of the harm they suffered: Plaintiffs and Class Members have no way of telling whether their PII that remains in Defendant's possession is actually secured, or whether it is vulnerable to another attack like that in the Data Breach.

**Personally Identifiable Information is Valuable to Cybercriminals**

86. In today's economy, the "world's most valuable resource is no longer oil, but data."[6] Indeed, an entire economy exists related to the value of personal data. In 2023 the big data technology market was valued at $349.40 billion in 2023 and is projected to grow to $397.27 in 2024.[7]

87. Because personal data is valuable personal property, legitimate market exchanges now exist where internet users like Plaintiffs and Class Members can sell or monetize their own personal data.

88. Thus, is not surprising that when malicious actors infiltrate companies and exfiltrate their stored PII, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[8] This same information is frequently sold and re-sold for years and years.

---

[6] *The World's Most Valuable Resource is No Longer Oil, but Data*, The Economist (May 6, 2017) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=17210591673&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=Cj0KCQjwlN6wBhCcARIsAKZvD5jiKx3uoiua5-6QWZUnZaabbTWzo37jSUU-qnsf3Km8qT9hFreCe8IaAhS9EALw_wcB&gclsrc=aw.ds

[7] *Big Data Technology Market Research Report*, Fortune Business Insights (Mar. 2024) https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144.

[8] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020,

89. Law enforcement has difficulty policing the dark web due to encryption which allows users and criminals to conceal identities and online activity.

90. Such PII is valuable on the dark web. For example, discrete pieces of personal information can be sold from $40 to $200, while bank details have a price range of $50 to $200.[9] Likewise, a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Passports can go for $1000 to $2000.[11] Cybercriminals can even purchase access to entire company data breaches.[12]

91. Once cybercriminals access a victim's PII, they can use it to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

92. Cybercriminals can also use this information to siphon money from accounts, open new accounts in the names of the victims, or sell the consumers' PII to someone else who will do the same.

93. The United States Government Accountability Office noted in a report on data breaches (the "GAO Report") that criminals can also use PII to receive government benefits and make purchases and secure credit in the victim's name. This type of identity fraud is the most

available at: https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Mar. 31, 2024).

[9] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Mar. 31, 2024).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 31, 2024).

[11] *Id.*

[12] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last visited Mar. 31, 2024).

harmful because it could take months or years for the victim to become aware of it, and it can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face 'substantial costs and inconveniences repairing damages to their credit records . . . [and their] good name."[13]

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

95. The lucrative value of such PII on the dark web has only led to increased instances of data breaches. Indeed, in 2023 the number of reported data breaches in the United States increased by 78%.[14]

96. In 2023, financial services companies such as Defendant "reported more than double the number of compromises compared to 2022."[15]

97. Because financial services companies are the frequent targets of cyberattacks, and because the PII Defendant collected, maintained, and stored in its systems is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties (such as identity theft or fraud), Defendant knew or should have known that it was a likely target of a cyberattack and would have been aware of the magnitude of harm its customers could face.

---

[13] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), *available at* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gao.gov/assets/gao-07-737.pdf (last visited Mar. 31, 2024).

[14] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, Infosecurity Magazine (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited Mar. 31, 2024).

[15] *Id.*

98. In addition to its obligations under federal and state laws, by way of their professional relationship, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII and financial information of Representative Plaintiffs and Class Members—and they failed to uphold that duty.

**Whitley Penn Failed to Comply with Regulatory Requirements and Standards**

99. Federal and state regulators have established security standards and issued recommendations to counter and avoid data breaches, the harm to consumers and the financial services sector.

100. For example, at least 24 states (including Texas, Virginia, New York, and California) have enacted laws addressing data security practices that require businesses that own, license, or maintain PII about a resident of that state to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access.

101. The Federal Trade Commission (FTC) has issued several guides for businesses regarding the importance of data security measures. According to the FTC, the need for data security should be considered for all business decision-making.[16]

102. In one set of guidelines, the FTC recommends that businesses use an intrusion detection system to discovery a breach as soon as it happens, monitor incoming traffic for activity

[16] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Mar. 31, 2024).

indicating someone is trying to hack their system, watch for large amounts of data being siphoned from a business' systems, and have a response plan should there be a data breach.[17]

103. In another guide, the FTC recommends that businesses should safeguard customer PII they retain, properly dispose of unnecessary PII, encrypt PII stored on computer networks, understand their network's vulnerabilities, and implement policies to rectify security issues.[18]

104. The FTC also recommends that businesses have a comprehensive communication plan that reaches all affected audiences in the event of a data breach. This plan should be designed to quickly notify people that their personal information has been compromised so that they can take steps to reduce the chance that their information will be misused, such as by changing passwords and putting a freeze on their credit reports. Timely notifications also make impacted consumers more vigilant and aware of potential phishing attempts.

105. The FTC further instructs businesses to provide detailed notices to affected parties that "clearly describe what you know about the compromise." This information, at a minimum, should include: "how it happened; what information was taken; how the thieves have used that information (if you know); what actions you have taken to remedy the situation; what actions you are taking to protect individuals, such as offering free credit monitoring services; and how to reach the relevant contacts in your organization."[19]

---

[17] *Id.*

[18] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Mar. 31, 2024)

[19] FTC, *Data Breach Response: A Guide for Business*, at 6, available at https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed April 11, 2024).

106. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

107. Whitley Penn's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

108. Whitley Penn's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

**Whitley Penn Failed to Comply with Industry Standards**

109. Cybersecurity firms have promulgated a series of best practices that should be consulted by and implemented when developing an organization's cybersecurity provisions. The Center for Internet Security released its Critical Security Controls which identify the most commonplace and essential cyber-attacks that affect businesses and proposes solutions to consult against those cyberattacks.[20] Organizations that collect and handle PII, such as Whitley Penn, are strongly encouraged to follow these controls.

110. These security controls include: securely configuring business software; managing access controls and vulnerability to networks, systems, and software; maintaining network infrastructure; adopting data encryption while data is both in transit and at rest; and securing application software.[21]

[20] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Mar. 31, 2024).
[21] *Id.*

111. The frequency and prevalence of attacks makes it imperative for entities to monitor for exploits and attacks routinely and constantly, and regularly update their software and security procedures.

112. For companies that share information with third parties, the CIS recommends that PII only be shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.[22]

113. The CIS Benchmarks are the clear option of choice for worldwide auditors when advising organizations on addition of secure builds standard of governance and security initiatives, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITLL.[23]

114. Whitley Penn failed to follow those and other industry standards to adequately protect Plaintiffs' and Class Members' PII.

**The Data Breach Injured Plaintiffs and Class Members and Causes Them a Continuing Risk of Future Harm**

115. The ramifications of Whitley Penn's failure to secure Plaintiffs' and Class Members' PII are severe.

116. Identity theft is defined by the FTC as "a fraud committed or attempted using the identifying information of another person without authority."[24]

117. Identity thieves can use PII, such as that of Plaintiffs and Class Members that was compromised in the Breach to perpetuate a variety of crimes including immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture;

[22] *Id.*
[23] *See CIS Benchmarks FAQ*, CIS, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq (last visited Mar. 31, 2024).
[24] 17 C.F.R. § 248.201 (2013).

using the victim's information to obtain government benefits, fabricate identities, and filing a fraudulent tax return using the victims' information to obtain a fraudulent refund.[25]

118. Any one of these instances of identity theft can have devastating consequences for the victim, causes years of often irreversible damage to their credit scores, financial stability, and personal security.

119. Data breach victims are much more likely to become victims of identity theft and other types of fraudulent schemes versus people whose PII was not compromised.

120. The above stated harms were maximized by the fact that Whitley Penn waited three months to notify Plaintiffs and Class Members of the Breach: for months Plaintiffs and the Class Members were unable to take available precautions to prevent or mitigate the imminent harms they faced by unknowingly having their PII exposed to a malicious actor.

121. Further, cybercriminals often wait for several months or even years to use the PII they originally exfiltrated or purchased on the dark web from another cybercriminal. The GAO noted:

> [L] enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

122. This means that Plaintiffs and Class Members will face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

123. It is very likely that Plaintiffs' and Class Members' PII has already been leaked and sold on the dark web.

---

[25] *Supra* n. 3.
[26] *Supra* n. 13 [GAO report] at 29.

124. Future identity theft is imminently and certainly pending due to the value of the information lost in this case which includes full names, addresses, birth dates, Social Security numbers, driver's license numbers, passport numbers, K-1 visa information, taxpayer identification numbers, banking account information and PIN numbers.

125. The exposure of any PII can cause unexpected harms one would not normally associate with the type of information stolen. Cybercriminals aggregate PII from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing, and other methods. The resulting complete dossiers of PII are particularly prized among cybercriminals because they expose the victim to every manner of identity theft and fraud.

126. Social engineering refers to the various techniques used by threat actors to convince a target to reveal additional specific information or perform special actions.[27] One type of social engineering is spear phishing, where a malicious actor focuses on a specific target based on specific information known about them.

127. For example, if a malicious actor knows a specific target's bank account information, they could create a fraudulent communication to that individual pretending to be the bank seeking additional payment or action from the target, resulting in the victim unknowingly sharing further personal information (such as credit card or additional banking information) with that malicious actor.

128. Here, the PII that was leaked in the breach is often used for such spear phishing attacks.

[27] *What is Social Engineering?*, European Union Agency for Cybersecurity (available at https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering).

129. One study showed that targeted spear phishing increased the likelihood of the cybercriminal successfully tricking the victim by ten percent.[28]

130. Identity theft victims spend numerous hours and their own money repairing the negative impact to their credit.[29]

131. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[30]

132. Plaintiffs and Class Members who had their Social Security numbers exposed also must deal with the fact that those numbers cannot easily be replaced. To obtain a new Social Security number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Further, as the Social Security Administration warns:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other Private Information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same.

For some victims of identity theft, a new Social Security number creates additional problems. For example, if the old credit card information is not associated with the new Social Security number,

---

[28] Bullee, Jan-Willem, and Montoya, Lorena, *Spear phishing in organisations explained*, Information & Computer Security, Vo. 25, No. 5 (2017), pp 593-613, available at https://www.researchgate.net/publication/320207541_Spear_phishing_in_organisations_explained.

[29] *Victims of Identity Theft*, Bureau of Justice Statistics (2021) chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bjs.ojp.gov/document/vit21.pdf.

[30] 2018 Identity fraud: Fraud Enters a New Era of Complexity, JAVELIN, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited Mar. 31, 2024).

the absence of any credit history under the new number may make it more difficult for the victim to get credit.[31]

133. The impact of identity theft can have ripple effects, adversely impacting future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced impacted their ability to get credit cards and obtain loans, like student loans or mortgages. For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.[32]

134. It follows that identity theft exacts a severe emotional toll on its victims.

135. The 2017 Identity Theft Resource Center survey[33] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft
- 7% reported feeling suicidal

[31] *Identity Theft and Your Social Security number*, SOCIAL SECURITY ADMINISTRATION, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 31, 2024)
[32] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RESOURCE CENTER, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Mar. 31, 2024).
[33] *Id.*

136. The same survey reported that identity theft can cause physical symptoms in victims:

- 48.3% of respondents reported sleep disturbances.
- 37.1% reported inability to concentrate or lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 37% reported fearing for the financial safety of family members
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.
- 7% reported feeling suicidal

137. As a result of the Data Breach, Plaintiffs and Class Members have suffered or will suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including but not limited to the following:

a. Losing the inherent value of their PII;

b. Losing the value of Whitley Penn's implicit promises of adequate data security;

c. Identity theft and fraud resulting from the theft of their PII;

d. Costs associated with the detection and prevention of identity theft and unauthorized use of their medical and health insurance information;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Unauthorized charges and loss of use and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

g. Lowered credit scores resulting from credit inquiries following fraudulent activities;

h. Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance an annoyance of dealing with repercussions of the Data Breach; and

i. The continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or many unauthorized third parties.

138. The above stated harms were exacerbated by the fact that Whitley Penn waited three months to notify Plaintiffs and Class Members of the Breach: for months Plaintiffs and the Class Members were unable to take available precautions to prevent or mitigate the imminent harms they faced by unknowingly having their PII exposed to a malicious actor.

139. In addition to the foregoing, Plaintiffs have already suffered harm as a result of the Data Breach.

***Plaintiff Alex Lawrence's Experience***

140. Plaintiff Alex Lawrence only allowed Defendant to maintain, store, and use his PII because he believed that Defendant would use basic security measures to protect the same, such as requiring passwords and multi-factor authentication to access databases storing his PII.

141. When Plaintiff Alex Lawrence's PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Alex Lawrence suffered injury from a loss of privacy.

142. Plaintiff Alex Lawrence has been further injured by the damages and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This

information has inherent value that Plaintiff was deprived of when his PII was unlawfully exfiltrated by an unknown third party.

143. Plaintiff Alex Lawrence has received at least two notifications and alerts following the Data Breach that his private information is on the dark web.

144. Further, Plaintiff Alex Lawrence has experienced a marked increase in spam calls, particularly over the past six months.

145. The Data Breach has also caused Plaintiff Alex Lawrence to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his PII being placed in the hands of an unknown third party.

146. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Alex Lawrence to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

147. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Alex Lawrence to suffer stress, fear, and anxiety. Plaintiff Alex Lawrence worries about someone using his PII to gain access to his bank account and draining it: he moved to a new home in 2023 and completed major renovations to it, and he was aware that if someone were to have improperly accessed his account or utilized his credit, that would have created major issues. He is also worried that somebody could use his PII to gain access to other accounts containing sensitive information such as accounts with medical providers containing protected health information.

148. Plaintiff Alex Lawrence 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 future breaches.

***Plaintiff Amanda Lawrence's Experience***

149. Plaintiff Amanda Lawrence only allowed Defendant to maintain, store, and use her PII because she believed that Defendant would use basic security measures to protect the same, such as requiring passwords and multi-factor authentication to access databases storing her PII.

150. When Plaintiff Amanda Lawrence's PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Amanda Lawrence suffered injury from a loss of privacy.

151. Plaintiff Amanda Lawrence has been further injured by the damages and diminution in value of her PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her PII was unlawfully exfiltrated by an unknown third party.

152. Plaintiff Amanda Lawrence has received five notifications and alerts following the Data Breach that her private information is on the dark web.

153. Furthermore, Plaintiff Amanda Lawrence has experienced a marked increase in spam calls and text message as a result of the Data Breach. Towards the end of 2023 Plaintiff Amanda Lawrence was receiving upwards of 5 or 6 spam calls a day.

154. The Data Breach has also caused Plaintiff Amanda Lawrence to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of an unknown third party.

155. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Amanda Lawrence to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

156. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Amanda Lawrence to suffer stress, fear, and anxiety. Plaintiff Amanda Lawrence constantly worries about her savings and her credit score, and knows that compromise of the information included in this breach could put her in a dire situation. As a woman in her 30s, she has major life events ahead of her such as having children, completing additional renovations, or buying a car, and realizes that theft from her accounts or credit issues could impact her ability to do those things.

157. Plaintiff Amanda Lawrence 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 future breaches.

***Plaintiff Nordstrom's Experience***

158. Plaintiff Nordstrom only allowed Defendant to maintain, store, and use his PII because he believed that Defendant would use basic security measures to protect the same, such as requiring passwords and multi-factor authentication to access databases storing his PII.

159. When Plaintiff Nordstrom's PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Nordstrom suffered injury from a loss of privacy.

160. Plaintiff Nordstrom has been further injured by the damages and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This

information has inherent value that Plaintiff was deprived of when his PII was unlawfully exfiltrated by an unknown third party.

161. Since the Data Breach, Plaintiff Nordstrom has received at least one notification that his information is on the dark web.

162. Further, Plaintiff Nordstrom has noticed a marked increase in spam calls and text messages following the Data Breach.

163. The Data Breach has also caused Plaintiff Nordstrom to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his PII being placed in the hands of an unknown third party.

164. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Nordstrom to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction. Additionally, because of the Data Breach, Plaintiff Nordstrom purchased software to scrub his private information from the internet.

165. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Nordstrom to suffer stress, fear, and anxiety. Plaintiff Nordstrom worries about suffering credit fraud, identity theft, or disclosure of his private information.

166. Plaintiff Nordstrom 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 future breaches.

***Plaintiff Raphael's Experience***

167. Plaintiff Raphael only allowed Defendant to maintain, store, and use his PII because he believed that Defendant would use basic security measures to protect the same, such as requiring passwords and multi-factor authentication to access databases storing his PII.

168. When Plaintiff Raphael's PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Raphael suffered injury from a loss of privacy.

169. Plaintiff Raphael has been further injured by the damages and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was unlawfully exfiltrated by an unknown third party.

170. Plaintiff Raphael has received an increased amount of spam text messages since the Data Breach.

171. The Data Breach has also caused Plaintiff Raphael to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his PII being placed in the hands of an unknown third party.

172. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Raphael to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

173. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Raphael to suffer stress, fear, and anxiety. Plaintiff Raphael worries about the fact that his personal information and banking information are no longer within his control.

174. Plaintiff Raphael 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 future breaches.

***Plaintiff Patel's Experience***

175. Plaintiff Patel only allowed Defendant to maintain, store, and use her PII because she believed that Defendant would use basic security measures to protect the same, such as requiring passwords and multi-factor authentication to access databases storing her PII.

176. When Plaintiff Patel's PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Patel suffered injury from a loss of privacy.

177. Plaintiff Patel has been further injured by the damages and diminution in value of her PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her PII was unlawfully exfiltrated by an unknown third party.

178. Plaintiff Patel has received three notifications and alerts following the Data Breach that her private information is on the dark web, including her social security number.

179. Furthermore, Plaintiff Patel has experienced a marked increase in spam calls as a result of the Data Breach.

180. The Data Breach has also caused Plaintiff Patel to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of an unknown third party.

181. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Patel to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

182. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Patel to suffer stress, fear, and anxiety. Plaintiff Patel worries about the unknown level of exposure and risk she faces now that her PII has been accessed by an unauthorized person and that there is no telling how long she will be at a heightened risk for exposure.

183. Plaintiff Patel 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 future breaches.

**Plaintiffs and Class Members Value Their Data Security**

184. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, firms like Whitley Penn would have no reason to tout their data security efforts to their actual and potential customers.

185. Consequently, had customers including Plaintiffs and Class Members known the truth about Whitley Penn's data security practices—that the firm would not adequately protect and store their data—they would not have entrusted their PII to their respective employers (if applicable) to then transfer to Whitley Penn, engaged Whitley Penn's accounting services, or paid as much for such services or benefits.

## CLASS ACTION ALLEGATIONS

186. Plaintiffs restate of the allegations in the preceding paragraphs as if set forth fully herein.

187. Pursuant to Tex. R. Civ. P. Rule 42, Plaintiffs bring this action individually and on behalf of the following Classes:

**Nationwide Class**

All persons residing in the United States whose PII was compromised in the Data Breach.

**California Subclass**

All persons residing in California whose PII was compromised in the Data Breach.

**New York Subclass**

All persons residing in New York whose PII was compromised in the Data Breach.

**Texas Subclass**

All persons residing in Texas whose PII was compromised in the Data Breach.

**Virginia Subclass**

All persons residing in the Commonwealth of Virginia whose PII was compromised in the Data Breach.

188. Plaintiffs represent, and are members of, this Class and Subclasses (together, the "Classes").

189. Excluded from the Classes are the Defendant, any entities in which Defendant has a controlling interest, the Defendant's employees, any Judge to whom this action is assigned, and any member of such Judge's staff and immediate family.

190. Plaintiffs reserve the right to amend or modify the Class and Subclass definitions after having an opportunity to conduct discovery.

191. The Classes meet the criteria for certification under Rule 42(a), (b)(2), (b)(3), and (c)(4). Plaintiffs and all members of the Classes have been harmed by the acts of the Defendant. Class-wide adjudication of Plaintiffs' claims is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

192. **Numerosity. Tex. R. Civ. P 42(a)(1).** The members of the Classes are so numerous that individual joinder of all Class Members is impracticable. Although the exact number of members is unknown at this time, it can readily be determined from the internal business records of Defendant, and Class members may be notified of the pendency of this action by published and/or mail/emailed notice. Plaintiffs reasonably estimate that there are hundreds of members of the Classes.

193. **Commonality and Predominance. Tex. R. Civ. P. 42(a)(2) and (b)(3).** Common questions of law and fact exist as to all members of the putative classes that will drive the litigation and predominate over any questions affecting only individual Class Members. Common questions include, but are not limited to:

A. Whether Defendant engaged in the conduct alleged herein;

B. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII from unauthorized access and disclosure;

C. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' PII violated state laws and/or the FTC Act, and/or Defendant's other duties discussed herein;

D. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

E. Whether Defendant unlawfully shared, lost, or disclosed Plaintiffs' and Class Members' PII;

F. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

H. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

I. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

J. Whether Defendant breached duties to protect Plaintiffs' and Class Members' PII;

K. Whether Defendant's actions and inactions alleged herein were negligent;

L. Whether Defendant was unjustly enriched by their conduct as alleged herein;

M. Whether an implied contract exited between Class Members and Defendant with respect to protecting PII and privacy, and whether that contract was breached;

N. Whether Plaintiffs and Class Members are entitled to actual and/ or statutory damages or other relief, and the measure of such damages and relief;

O. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief;

P. Whether Plaintiffs and the Class Members are entitled to equitable relief, including restitution, injunctive relief, and/or disgorgement and the proper measure of such relief.

194. **Typicality. Tex. R. Civ. P. 42(a)(3).** Plaintiffs' claims are typical of the claims of each putative class member and are based on the same facts and legal theories as each of the Class

Members. Plaintiffs, like all members of the Classes, entrusted their PII to Defendant, either directly or through their employers, and Plaintiffs, like all Class Members, had their PII compromised as a result of Defendant's negligence. Plaintiffs are entitled to relief under the same causes of action as the other members of the putative classes.

195. **Adequacy of Representation. Tex. R. Civ. P. 42(a)(4).** Plaintiffs are adequate representatives of the putative Classes because their interests coincide with, and are not antagonistic to, the interests of the members of the Classes that they seek to represent. Plaintiffs have retained counsel competent and highly experienced in complex consumer class action litigation, who intend to prosecute the action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the members of the Classes.

196. **Superiority. Tex. R. Civ. P. 42(b)(3).** Questions of law and fact common to the Classes predominate over questions affecting only individual members, and a class action is superior to other available methods for fair and efficient adjudication of the controversy. The damages sought by each member are /such that individual prosecution would prove burdensome and expensive. It would be virtually impossible for members of the Classes individually to effectively redress the wrongs done to them. Even if the members of the Classes themselves could afford such individual litigation, it would be an unnecessary burden on the Courts. Furthermore, individualized litigation presents a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and to the court system presented by the legal and factual issues raised by Defendant's conduct. By contrast, the class action device will result in substantial benefits to the litigants and the Court by allowing the Court to resolve numerous individual claims based upon a single set of proof. Plaintiffs are not aware of any other current pending litigation against Defendant to which any Class Member is a party involving the subject

matter of this suit, and the Action presents no difficulties that will impede its management by the Court as a class action.

197. **Injunctive Relief Appropriate for the Class. Tex. R. Civ. P. 42(b)(2).** Class certification is appropriate because Defendant acted on grounds generally applicable to the Classes, thereby making appropriate injunctive relief and/or corresponding declaratory relief with respect to Plaintiff and putative Class Members. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual Class Members that could establish incompatible standards of conduct for Defendant. Injunctive relief is necessary to prevent further fraudulent and unfair business practices by Defendant.

## CAUSES OF ACTION

### FIRST CAUSE OF ACTION
### NEGLIGENCE
### (By Plaintiffs and on behalf of the Classes)

198. Plaintiffs restate and realleged the foregoing paragraphs above as if fully set forth herein.

199. Defendant's clients, including Plaintiffs' former employers, are required by Defendant to provide non-public PII as a condition of receiving tax and/or accounting services from Defendant.

200. Defendant required Plaintiffs and Class Members to provide their PII, and gathered and stored this PII as part of its business, which affects commerce.

201. Plaintiffs and Class Members entrusted Defendant with their PII with the reasonable understanding that Defendant would take adequate security precautions to safeguard their highly sensitive information.

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

203. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and prevent disclosure of the information to unauthorized third parties, to safeguard the information from theft, and to implement procedures to detect the loss or unauthorized dissemination of PII in its possession.

204. Defendant owed a duty of care to Plaintiffs and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks and the personnel responsible for them adequately protected the PII.

205. These duties arose as a result of the special relationship that existed between Defendant and the Plaintiffs and Class Members. The special relationship arose because Defendant, a sophisticated and experienced accounting firm, was entrusted with Plaintiffs and the Class Members' PII, a necessary part of the tax and accounting services Defendant provides.

206. Defendant also had a duty to promptly and adequately notify Plaintiffs and the Class Members of the Data Breach – and generally of any security incidents or intrusions that affected or may have affected their PII and financial information – but failed to do so.

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

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII and financial information in line with industry standards, despite the known, increasing threat to financial service companies;

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

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely matter that class Members' PII had been compromised;

e. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

209. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' PII would damage Plaintiffs and Class Members.

210. Defendant breached its duties to Plaintiffs and the Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members PII.

211. The FTC has pursued enforcement actions against businesses like Defendant, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiffs and the Class.

212. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's business as certified public accountants and its continuing education requirements in this field, which emphasize the necessity

and best practices for diligently protection of PII,[34] and in light of Defendant's inadequate security practices.

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

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

215. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

216. Plaintiffs and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

217. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach because Defendant could have prevented the Data Breach by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII and financial information.

218. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures.

219. Defendant's duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place

[34] See, e.g., a multitude of resources related to "data breach" on American Institute of Certified Public Accountants (https://www.aicpa.org/search/data+breach).

to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

220. Defendant admitted that Plaintiffs and Class Members' PII was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

221. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and the Class, Plaintiffs and Class Members' PII would not have been compromised.

222. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiffs and Class Members' PII, and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

223. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value

of ongoing credit monitoring and identity defense services necessitated by Defendant's data breach; (x) the value of the unauthorized access to their PII permitted by Defendant; and (xi) any nominal damages that may be awarded.

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

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

226. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiffs' and Class Members' PII in an unsafe and unsecure manner.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE *PER SE***
**(By Plaintiffs and on behalf of the Classes)**

227. Plaintiffs restate the foregoing paragraphs as if fully set forth herein.

228. Defendant had duties arising under multiple state statutes (including those enumerated below) and the FTC Act to protect Plaintiffs' and Class Members' PII.

229. For example, like several state consumer protection statutes, the FTC Act, Section 5, 15 U.S.C. §45, 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 PII and financial information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

230. Defendant breached its duties, pursuant to state law data security and consumer protection statutes and the FTC Act, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' PII; (iv) failing to detect in a timely manner that Class Members' PI had been compromised; and (v) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

231. Defendant's violation of various state data security and consumer protection statutes and the FTC Act (and similar state statutes) constitutes negligence *per se*.

232. Plaintiffs and Class Members are consumers within the class of persons that the FTC Act were intended to protect.

233. The harm that has occurred is the type of harm the state data security and consumer protection statutes and the FTC Act were intended to guard against.

234. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

235. In addition, under state data security and consumer protection statutes such as those outlined herein, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

236. Plaintiffs and Class Members were foreseeable victims of Defendant's violations of the state data security and consumer protection statutes and the FTC. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and the Classes.

237. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (vi) loss of benefit of the bargain; (vii) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

**THIRD CAUSE OF ACTION**
**BREACH OF THIRD PARTY BENEFICIARY CONTRACT**
**(By Plaintiffs and on behalf of the Classes)**

240. Plaintiffs restate the foregoing paragraphs as if fully set forth herein.

241. Upon information and belief, Defendant entered into contracts to provide services to its clients, which services included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be provided to it.

242. Upon information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiffs and the Class Members, as it was their PII that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

243. Defendant knew that if it were to breach these contracts with its clients, the clients' members, including Plaintiffs and the Class Members, would be harmed.

244. Defendant breached its contracts with its clients—whose beneficiaries, including Plaintiffs and the Class Members—were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiffs and Class Members regarding the Breach.

245. As was foreseeable, Plaintiffs and the Class Members were harmed by Defendant's failure to use reasonable data security measures to store the PII Plaintiffs and Class Members provided to Defendant, and were harmed by Defendant's failure to timely notify Plaintiffs and Class Members of the breach, subjecting them to a continuous and substantial risk of harm through the loss of their PII.

246. Accordingly, Plaintiffs and the Class Member are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

**FOURTH CAUSE OF ACTION**
**BREACH OF IMPLIED CONTRACT**
**(By Plaintiffs and on behalf of the Classes)**

247. Plaintiffs restate the foregoing paragraphs as if fully set forth herein.

248. Defendant offered to provide services to its clients, which are Plaintiffs and/or their employers, in exchange for payment.

249. Defendant required Plaintiff and Class Members to provide it with their PII in order to receive services.

250. In turn, Defendant impliedly promised to protect Plaintiffs' and Class Members' PII through adequate data security measures.

251. Plaintiffs and Class Members accepted Defendant's offer by providing their valuable PII to Defendant, or to their employers or other entities (if applicable) who in turn provided that information to Defendant in exchange for Plaintiffs and Class Members receiving Defendant's services, and then by paying for and receiving the same (payments which, upon information and belief, directly benefitted Defendant).

252. Plaintiffs and Class Members would not have done the foregoing but for the above described agreement with Defendant.

253. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant in exchange for, amongst other things, the protection of such information.

254. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

255. However, Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

256. In sum, Plaintiffs and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

257. Moreover, the covenant of good faith and fair dealing is an element of every contract. All such contracts impose on 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, meanings 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 along with its form.

258. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

259. As a direct and proximate result of Defendant' above-alleged breach of implied contract, Plaintiffs and Class Members have suffered and will continue to suffer: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen PII; (c) the illegal sale of the compromised PII on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit

freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work time; (j) the lost value of the PII; (k) the lost value of access to their PII permitted by Defendant; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach; (m) the lost benefit of their bargains and overcharges for services or products; and (n) nominal and general damages; and other economic and non-economic harm.

260. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages along with costs and attorneys' fees incurred in this action.

**FIFTH CAUSE OF ACTION**
**UNJUST ENRICHMENT**
**(*In the alternative*)**
**(By Plaintiffs and on behalf of the Classes)**

261. Plaintiffs restate the foregoing paragraphs as if fully set forth herein.

262. This count is pleaded in the alternative to the breach of third-party beneficiary contract claim (Third Cause of Action) and breach of implied contract claim (Fourth Cause of Action).

263. Plaintiffs and Class Members conferred a monetary benefit on Defendant in connection with obtaining accounting and/or tax services, specifically providing Defendant with their PII in exchange, Plaintiffs and Class Members should have received from Defendant services or benefits that were the subject of the transaction, and should have had their PII protected with adequate data security.

264. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

265. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

266. If Plaintiffs and Class Members had known Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, or vendors that house PII, they would not have entrusted their PII with Defendant.

267. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

268. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their PII, which: (a) remains available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by Defendant's Data Breach; (x) the value of the

unauthorized access to their PII permitted by Defendant; and (xi) any nominal damages that may be awarded.

269. Plaintiffs and Class Members are entitled to restitution and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

270. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to other claims pleaded herein.

## SIXTH CAUSE OF ACTION
## Va. Code Ann. §§ 59.1-196, *et seq.*
## (By Plaintiffs Alex Lawrence and Amanda Lawrence and on Behalf of the Virginia Subclass)

271. Plaintiffs Alex and Amanda Lawrence (the "Virginia Plaintiffs") restate the foregoing allegations as if fully set forth herein.

272. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

273. Defendant is a "person" as defined by Va. Code Ann. § 59.1-198.

274. Defendant is a "supplier," as defined by Va. Code Ann. § 59.1-198.

275. Defendant engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198.

Defendant advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

276. Defendant engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Virginia Plaintiffs' and Virginia 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 sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Virginia Plaintiffs' and Virginia 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 the Virginia Plaintiffs' and Virginia 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 the Virginia Plaintiffs' and Virginia 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 properly secure Virginia Plaintiffs' and Virginia 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 Virginia Plaintiffs' and Virginia Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

277. Defendant intended to mislead Virginia Plaintiffs and Virginia Subclass Members and induce them to rely on its misrepresentations and omissions.

278. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Virginia Plaintiffs and Virginia Subclass Members, about the adequacy of Defendant's computer and data security and the quality of the Defendant's brand.

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

280. Defendant had a duty to disclose these 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 Virginia Plaintiffs and the Virginia Subclass Members—and Defendant, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant'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, while purposefully withholding material facts from Virginia Plaintiffs and Virginia Subclass Members that contradicted these representations.

281. The above-described deceptive acts and practices also violated the following provisions of Va. Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain characteristics, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model;

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised;

d. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

282. Defendant acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Virginia Plaintiffs' and Virginia Subclass Members' rights. An award of punitive damages would serve to punish Defendant for its wrongdoing, and warn or deter others from engaging in similar conduct.

283. As a direct and proximate result of Defendant's deceptive acts or practices, Virginia Plaintiffs and Virginia 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 Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

284. Defendant's violations present a continuing risk to the Virginia Plaintiffs and Virginia Subclass Members as well as to the general public.

285. Virginia Plaintiffs and Virginia Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

**SEVENTH CAUSE OF ACTION**
**New York General Business Law § 349**
**(By Plaintiff Raphael and on behalf of the New York Subclass)**

286. Plaintiff Raphael restates the foregoing allegations as if fully set forth herein.

287. Plaintiff Raphael brings this claim on behalf of himself and the New York Subclass.

288. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Raphael's and the New York 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 sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Raphael's and New York 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 Raphael's and New York 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 Raphael's and New York 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 properly secure Plaintiff Raphael's and New York 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 Raphael's and New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

290. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff Raphael's and New York Subclass Members' rights.

291. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff Raphael and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged 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; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

292. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

293. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff Raphael and New York Subclass Members that they could not reasonably avoid.

294. Plaintiff Raphael and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

**EIGHTH CAUSE OF ACTION**
**California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.***
**(By Plaintiff Nordstrom and on behalf of the California Subclass)**

295. Plaintiff Nordstrom restates the foregoing allegations as if fully set forth herein.

296. Plaintiff Nordstrom and the California Subclass Members are residents of California.

297. Defendant is a limited liability partnership organized or operated for the profit or financial benefit of its owners. Defendant collects consumers' "Personal Information" and "Sensitive Personal Information" as defined in the California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140.

298. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff Nordstrom's and California Subclass Members' nonencrypted Personal Information and Sensitive Personal Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

299. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Nordstrom's and California Subclass Members' Personal Information and Sensitive Personal Information. As detailed herein, Defendant failed to do so.

300. As a direct and proximate result of Defendant's acts, Plaintiff Nordstrom's and California Subclass Members' Personal Information and Sensitive Personal Information, including

names, social security numbers, bank account information, dates of birth, and other sensitive information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

301. Plaintiff Nordstrom and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter properly safeguards customer Personal Information and Sensitive Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customer Personal Information and Sensitive Personal Information, including Plaintiff Nordstrom's and California Subclass Members' Personal Information and Sensitive Personal Information. Plaintiff Nordstrom and California Subclass Members have an interest in ensuring that their Personal Information and Sensitive Personal Information is reasonably protected.

302. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

303. On July 17, 2024, counsel for Plaintiff Nordstrom provided written notice via certified mail to Defendant at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for Defendant to cure. Defendant received the written notice. Plaintiff Nordstrom's written notice set forth the violations of Defendant's duty to implement and maintain reasonable security procedures and practices alleged in this Petition.

304. If, within thirty days after Plaintiff Nordstrom's written notification, Defendant fails to provide appropriate relief for its violations of the CCPA, Plaintiff will amend this Petition to seek actual damages. To date, Defendant has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff Nordstrom's counsel.

305. Plaintiff Nordstrom and the California Subclass seek all monetary and non-monetary relief allowed by law, including injunctive relief and any other equitable relief the Court deems proper as well as costs and reasonable and necessary attorneys' fees.

**NINTH CAUSE OF ACTION**
**California Consumer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.***
**(By Plaintiff Nordstrom and on Behalf of the California Subclass)**

306. Plaintiff Nordstrom restates the foregoing allegations as if fully set forth herein.

307. Plaintiff Nordstrom and the California Subclass Members are residents of California.

308. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

309. Defendant is a business that owns, maintains, and licenses personal information within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiff Nordstrom and California Subclass Members. Plaintiff and California Subclass Members' PII includes "personal information as covered by Cal. Civ. Code § 1798.82.

310. Businesses that own or license computerized data that includes personal information are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the

types of personal information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

311. Because Defendant reasonably believed that Plaintiff Nordstrom's and California Subclass Members' personal information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

312. As discussed above, Defendant failed to disclose material information about the Data Breach and further failed to disclose the Data Breach in a timely and accurate manner in violation of Cal Civ. Code § 1798.82.

313. Defendant also violated Cal. Civ. Code § 1798.82 by not publishing a notice of data breach in the format required by Cal. Civ. Code § 1798.82(d)(1).

314. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Nordstrom and California Subclass Members suffered damages, as alleged above.

315. Plaintiff Nordstrom and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

**TENTH CAUSE OF ACTION**
**California Unfair Competition Act, Cal. Bus. & Prof. Code §§ 17200 *et seq.***
**(By Plaintiff Nordstrom and on behalf of the California Subclass)**

316. Plaintiff Nordstrom restates the foregoing allegations as if fully set forth herein.

317. Plaintiff Nordstrom and the California Subclass Members are residents of California.

318. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

319. Defendant violated Cal. Bus. & Prof. Code §§ 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

320. Defendant's unfair acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff Nordstrom and California Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security risks and remediate identified security risks as alleged herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Nordstrom and California Subclass Members, whose PII has been compromised;

c. Failing to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100;

d. Failing to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as alleged above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Defendant's grossly inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

e. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

321. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code. §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and California common law.

322. Defendant's unlawful, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Nordstrom's and California 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 sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Nordstrom's and California 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 Nordstrom's and California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff Nordstrom's and California Subclass Members' PII;

f. 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 Nordstrom's and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

g. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

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

324. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff Nordstrom and California Subclass Members were injured and suffered monetary and non-monetary damages, as alleged 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; loss of the value of access to their PII; and the value of identity protection and/ or data protection services made necessary by the Data Breach.

325. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Nordstrom's and California Subclass Members' rights.

326. Plaintiff Nordstrom and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

## ELEVENTH CAUSE OF ACTION
## Deceptive Trade Practices – Consumer Protection Act, Texas Bus. & Com. Code §§ 17.41 *et seq.*
## (By Plaintiff Patel and on behalf of the Texas Subclass)

327. Plaintiff Patel restates the foregoing allegations as if fully set forth herein.

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

329. Defendant is a "person" as defined by the Texas Trade Practices-Consumer Protection Act ("DTPA"), Tex. Bus. & com. Code § 17.45(3).

330. Defendant 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).

331. Defendant 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;

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.

332. Defendant's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable privacy measures to protect Plaintiff Patel's and Texas 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 sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

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

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff Patel's and Texas 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 Patel's and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052.

333. Defendant intended to mislead Plaintiff Patel and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

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

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

336. Defendant had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent 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 Patel and Texas Subclass Members, and Defendant because consumers are

unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of 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, while purposefully withholding material facts from Plaintiff Patel and Texas Subclass Members that contradicted these representations.

337. Defendant engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 1750(a)(3). Defendant 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.

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

339. Defendant 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 Defendant's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Defendant's unconscionable business acts and practices, exposed Plaintiff Patel and Texas Subclass Members to a wholly

unwarranted risk to the safety of their PII and the security of their identity or credit, and caused a substantial hardship on a significant and unprecedented number of consumers. Plaintiff Patel and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

340. Defendant acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff Patel's and Texas Subclass Members' rights.

341. As a direct and proximate result of Defendant's unconscionable and deceptive acts or practices, Plaintiff Patel and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as alleged 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 Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach. Defendant's unconscionable and deceptive acts or practices were a producing cause of Plaintiff Patel's and Texas Subclass Members' injuries, ascertainable losses, economic damages, and noneconomic damages, including their mental anguish.

342. Defendant's violations present a continuing risk to Plaintiff Patel and the Texas Subclass Members, as well as to the general public.

343. Contemporaneous with the filing of this Petition, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiff's counsel will send to the Consumer Protection Division a copy of the written notice sent to Defendant.

344. On July 17, 2024 and March 13, 2025, counsel for Plaintiff Patel provided written notice via certified mail to Defendant at its principal place of business of the intent to pursue claims under the DTPA and an opportunity for Defendant to cure. Plaintiff's written notice sets forth the violations of Defendant's duty to implement and maintain reasonable security procedures and practices alleged in this Petition.

345. Plaintiff Patel and the Texas Subclass Members seek damages, including economic damages, damages for mental anguish, statutory damages in the amount of three times the economic and mental anguish damages, as Defendant's acts were committed intentionally or knowingly, injunctive relief, and any other equitable relief the Court deems proper, as well as costs and reasonable and necessary attorneys' fees.

## PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Defendant Whitley Penn as follows:

- Certifying the Classes as requested herein, designating Plaintiffs as Class and Subclass representatives, and appointing Plaintiffs' counsel as Class Counsel;

- Awarding Plaintiffs and the Classes appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

- Awarding Plaintiffs and the Classes equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

- Awarding Plaintiffs and the Classes pre-judgment and post-judgment interest to the maximum extent allowable;

- Awarding Plaintiffs and the Classes reasonable attorneys' fees, costs, and expenses, as allowable; and

- Awarding Plaintiffs and the Classes such other favorable relief as allowable under law.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury on all triable issues.

DATED: March 17, 2025

Respectfully submitted,

*/s/ Shana H. Khader*

Shana H. Khader (TX State Bar No. 24099860)
Gemma Seidita*
**TYCKO & ZAVAREEI LLP**
2000 Pennsylvania Ave., NW Suite 1010
Washington, District of Columbia 20006
(202) 973-0900
*skhader@tzlegal.com*
*gseidita@tzlegal.com*

*Application for admission *pro hac vice* forthcoming

*Counsel for Plaintiffs and the Proposed Classes*

# Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Linda Zhu on behalf of Shana Khader
Bar No. 24099860
lzhu@tzlegal.com
Envelope ID: 98554648
Filing Code Description: Petition
Filing Description:
Status as of 3/17/2025 5:49 PM CST

Case Contacts

| Name | BarNumber | Email | TimestampSubmitted | Status |
|---|---|---|---|---|
| Michelle Gomez | | mgomez@bakerlaw.com | 3/17/2025 5:29:51 PM | SENT |
| Shana Khader | | skhader@tzlegal.com | 3/17/2025 5:29:51 PM | SENT |
| Gemma Seidita | | gseidita@tzlegal.com | 3/17/2025 5:29:51 PM | SENT |
| Sabita Soneji | | ssoneji@tzlegal.com | 3/17/2025 5:29:51 PM | SENT |

# EXHIBIT 1

2024-413

<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<Name 1>>
<<Name 2>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

<<Maildate>>

**Notice of Data Breach**

Dear <<Name 1>>,

**What Happened**

We are writing to inform you of an incident that involved your personal information. On October 31, 2023, we identified suspicious activity within a certain Whitley Penn email account. Upon learning of this incident, we immediately took steps to secure our network and launched an investigation in coordination with third-party forensic specialists to determine the nature and scope of the activity. After a thorough investigation, on November 21, 2023, we determined that certain data used in the preparation of your tax return may have been exposed as a result of a malicious cyberattack.

We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident.

**What Information Was Involved**

Although the specific information contained within the account in question varies by individual, the account may have contained certain data used in the preparation of your tax return, such as first and last name, address, date of birth, driver's license number, passport number, Social Security number, K-1 visa information, taxpayer identification number, banking account information, PIN number, and/or certain financial information.

**What We Are Doing**

We take the confidentiality, privacy, and security of information in our possession seriously, and we have security measures in place to help protect the information we collect. Upon learning of this incident, we promptly notified law enforcement and commenced the forensic investigation referenced above. Additionally, as part of our ongoing commitment to protecting the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further secure the information in our systems. We also worked with the third-party subject matter specialists to further enhance the security of our systems and prevent future attacks.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks$^{SM}$ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Ensure that you enroll by April 4, 2024** (Your code will not work after this date.)
- **Visit the Experian IdentityWorks website to enroll**: https://www.experianidworks.com/3bcredit
- **Provide your activation code**: **<<Activation Code>>**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by April 4, 2024. Be prepared to provide engagement number **<<Engagement #>>** as proof of eligibility for the Identity Restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**What You Can Do**

The events that have occurred do not automatically mean that you are a victim of identity theft. However, we encourage you to remain vigilant, to continually review your credit report, bank account activity, and bank statements for irregularities or unauthorized items, and to immediately report any unauthorized charges to your financial institution.

We also encourage you to contact Experian with any questions and to enroll in the free identity protection services by calling 1-877-288-8057, going to https://www.experianidworks.com/3bcredit. Please note the deadline to enroll is April 4, 2024. Again, at this time, we are not aware of any evidence indicating that your information has been misused. However, we encourage you to take full advantage of this service offering.

**What is Whitley Penn**

Whitley Penn is a Texas-based, full-service accounting and advisory firm with a global reach through its affiliation with another entity. If you received this letter, you are/were previously a client of Whitley Penn or are/were an employee of one of Whitley Penn's clients.

**For More Information**

When calling or enrolling online for Experian IdentityWorks, you will need to reference the Experian enrollment code provided, so please do not discard this letter. The specific instructions are above.

We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident. Please call 888-368-6235 if you'd like to speak to someone regarding any additional questions you may have.

Sincerely,

Toby Cotton
Tax Practice Leader
Whitley Penn

## Information About Identity Theft Protection

### Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. Under U.S law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax®**
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

**Experian**
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

**TransUnion®**
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

### Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

**Equifax**
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

**Experian**
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

**TransUnion**
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Copy of a government-issued identification card;
7) A copy of a police report or other complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft; and
8) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

**Fraud Alerts**

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105788 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5788 | Allen, TX 75013-9554 | Chester, PA 19016-2000 |
| 1-888-766-0008 | 1-888-397-3742 | 1-800-680-7289 |
| www.equifax.com/personal/credit-report-services | www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert |

**Monitor Your Personal Health Information**

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

**New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

**North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.