

067-333679-22
CAUSE NO. _____

FILED
TARRANT COUNTY
5/20/2022 3:05 PM
THOMAS A. WILDER
DISTRICT CLERK

DENNIS TARRANT, individually and
on behalf of all others similarly situated,

Plaintiff,

v.

SOUTHLAND HOLDINGS LLC,

Defendant.

§
§
§
§
§
§
§
§

IN THE DISTRICT COURT

_____ JUDICIAL DISTRICT

TARRANT COUNTY, TEXAS

PLAINTIFF'S ORIGINAL PETITION IN CLASS ACTION

TABLE OF CONTENTS

DISCOVERY CONTROL PLAN 1

PARTIES 1

JURISDICTION AND VENUE 3

STATEMENT OF FACTS 3

 A. Defendant’s Business Practices 3

 B. The Breach of Security 6

 C. The Defendant’s Untimely Notification of The Breach of Security to the Victims 8

 D. Plaintiff Dennis Tarrant’s Experience 10

 E. The Value of Personally Identifiable Information 12

 F. Laws and Industry Customs and Standards that Underscore Defendant's Duty to
 Implement Reasonable Information Security Practice. 17

 G. Plaintiff and Class Members Have and Will Continue to Be Harmed as a
 Consequence of Defendant’s Information-Security Failures and Tortious Conduct. 23

CLASS ACTION ALLEGATIONS 26

CAUSES OF ACTION 30

 Count I: Negligence 30

 Count II: Breach Of Contract..... 34

 Count III: Breach Of Confidence.....**Error! Bookmark not defined.**

 Count IV: Invasion Of Privacy 36

 Count V: Unjust Enrichment 38

DAMAGES OR EQUITABLE REMEDIES 39

JURY DEMAND 40

PRAYER FOR RELIEF 40

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff Dennis Tarrant, individually and on behalf of all others similarly situated, by and through their undersigned counsel, files this petition against Defendant Southland Holdings LLC (“Defendant” or “Southland”), a Texas limited liability company, and alleges, upon personal knowledge as to his own actions and his counsels’ investigations, and upon information and belief as to all other matters, as follows:

DISCOVERY CONTROL PLAN

1. Plaintiff pleads that discovery should be conducted in accordance with a Level 3 discovery control plan under Tex. R. Civ. P. 190.3.

PARTIES

2. Plaintiff Dennis Tarrant (hereinafter “Plaintiff” or “Plaintiff Tarrant”) is an individual citizen of the State of Texas residing, and at all times pertinent to this action has resided, in Greenville, Hunt County, Texas.

3. At Defendant’s request, Plaintiff entrusted sensitive, personal, and private information that was compromised, unlawfully accessed, and stolen due to Defendant Southland’s misconduct as described below.

4. On or around April 8, 2022, Plaintiff Tarrant received a letter entitled “Notice of Data Security Incident”¹ in which Defendant acknowledged that it experienced a targeted cyberattack where the perpetrators gained unauthorized access to Plaintiff’s sensitive personal information, including unencrypted name, address, Social Security number, and driver’s license number (the “Data Breach”).

¹ A true and correct copy of Southland’s “Notice of Data Security Incident” is attached as Exhibit A.

5. Plaintiff brings this action against Defendant to hold it accountable for the harm it caused Plaintiff and at least 5,027 similarly situated individuals (“Class Members”) as a result of the Defendant’s failure to take reasonable precautions to protect from unauthorized and unlawful use or disclosure the sensitive personal information that it collects and maintains in the regular course of business.

6. Defendant is a domestic limited liability company registered to do business under the laws of the State of Texas, with its principal place of business located at 1100 Kubota Drive, Grapevine, TX 76051.

7. Defendant may be served by mailing a true and correct copy of the citation with this petition, including its attachments, by U.S. certified mail, return receipt requested, to Defendant’s agent for service of process in this State, Southland Contracting, Inc., at the following address: 608 Henrietta Creek Rd., Roanoke, TX 76262.

8. Defendant operates as a holding company and is the parent company of Johnson Bros. Corporation, American Bridge Company, Oscar Renda Contracting, Defendant Contracting, Mole Constructors, and Heritage Materials.

9. All of the claims stated in this petition are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

10. Defendant is a commercial entity that routinely collects and maintains personally identifiable information and personal health information from individual employees in connection with its business activities.

JURISDICTION AND VENUE

11. This Court has jurisdiction over the present case because this matter involves claims in excess of the minimum and otherwise within the Court's jurisdictional limits, and it involves causes of action over which this Court has subject matter jurisdiction.

12. Plaintiff seeks monetary relief of over \$1,000,000 and non-monetary relief.

13. Venue is proper in Tarrant County, Texas under Tex. Civ. Prac. & Rem. Code § 15.002(a) because this was the county in which a substantial part of the events and omissions giving rise to the claims occurred.

14. Additionally, venue is proper in Tarrant County, Texas because Defendant's principal office is located in Tarrant County. Tex. Civ. Prac. & Rem. Code Ann. § 15.002(a)(3).

15. This action is brought by Plaintiff as a class action on his own behalf, and on behalf of all others similarly situated, under Rule 42 of the Texas Rules of Civil Procedure. Plaintiff seeks damages, injunctive, declaratory relief and incident and subordinate relief, including costs.

STATEMENT OF FACTS

A. Defendant's Business Practices

16. According to its website, Defendant Southland is one of the largest construction companies in North America.² Through its subsidiaries, Defendant offers infrastructure construction and civil engineering services to the transportation, tunneling, heavy civil, bridges and structures, water treatment facilities and conveyance, alternate delivery, and engineering markets.

²<https://www.southlandholdings.com/our-history/> (last visited May 2, 2022).

17. As a condition of and during the course of employment, Defendant requires that its employees, including job applicants (collectively, “employees”) disclose information that alone or in conjunction with other information identifies an them, including contact information (including postal addresses, email addresses, and phone numbers); Social Security numbers (SSNs), dates of birth, and driver’s license numbers or government-issued identification numbers (collectively “Personally Identifying Information” or “PII”).

18. On information and belief, in the course of collecting PII from prospective, current and former employees, Defendant promised to provide confidentiality and adequate security for employee data through their applicable privacy policy and through other disclosures.

19. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business and/or employment purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

20. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep client, consumer, and employee PII safe and confidential.

21. As a condition of their employment, Plaintiff and Class Members were obligated to provide Defendant with their PII.

22. Defendant derived a substantial economic benefit from collecting Plaintiff’s and Class Members’ PII.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

24. Plaintiff and Class Members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe.

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep this information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

26. Plaintiff and Class Members reveal their PII to Defendant with the understanding, whether express or implicit, that Defendant will keep the information confidential and not share or disclose it without the employee's consent in the absence of legitimate business reasons for doing so.

27. Defendant holds itself out as respecting individuals' privacy to gain the trust of those it employs and individuals who use its products or service.

28. Defendant causes employees to reasonably believe that it will not disclose their personal data based on reasonable social expectations.

29. Defendant's legal obligations and the express and implied representations it made concerning its information privacy and security practices would lead a reasonable person in similar circumstances to believe that Defendant had in place reasonable procedures to protect from

unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

30. No reasonable person, including Plaintiff, would have provided their PII without an understanding that Defendant would take reasonable steps to protect that information consistent with its promises, its legal obligations, and the implied terms of its express contracts.

31. Plaintiff and Class Members were employees of Defendant whose PII was required to be provided, and was in fact provided, to Defendant in conjunction with hiring or during the course of their employment with Defendant.

32. Plaintiff and Class Members relied on Defendant's superior knowledge, skill, and sophistication to safeguard the confidentiality and integrity of their PII.

33. Defendant failed to disclose the material fact that it did not have in place reasonable procedures to protect the sensitive personal information it collected from unlawful use or disclosure.

34. Had Defendant disclosed this material fact, Plaintiff and Class Members would not have entrusted their PII to Defendant.

B. The Data Breach

35. Hackers exploited Defendant's cybersecurity vulnerabilities to steal and monetize the information Defendant collected, including Plaintiff's and Class Members' PII.

36. On or about September 21, 2021, Defendant discovered that its IT environment and network was under attack by unauthorized threat actors.

37. During the investigation of the breach of security, Defendant also uncovered that the hackers found and accessed sensitive personal information stored on Defendant's network.

38. The compromised information included the unencrypted names, addresses, Social Security numbers, and driver's license numbers belonging to 5,207 citizens of Texas, including Plaintiff and Class Members.

39. Upon information and belief, the compromised information was posted on file-sharing websites for identity thieves to download, sell on the black market, and use to send emails, phone calls, solicit, and harass, Defendant's employees and their families.

40. The compromised information has already been used to commit identity theft and/or fraud.

41. The compromised information remains unencrypted and available for unauthorized third parties to access and abuse; and may remain 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.

42. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

43. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

44. In light of recent high-profile data breaches at other companies similar to Defendant, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

C. The Defendant's Untimely Notification of The Breach of Security to the Victims

45. Following the Data Breach, Defendant unreasonably delayed notifying the victims about the nature and scope of the breach and what steps Defendant was taking to remedy or mitigate the breach.

46. On or about April 8, 2022, nearly seven months after discovering the Data Breach, Defendant sent a Notice of Data Security Incident letter (the "Notice") to affected individuals, including Plaintiff, acknowledging the cyberattack. *See Exhibit A.*

47. The Notice also stated that Defendant retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident, and that it reported the breach to the Federal Bureau of Investigations.

48. The Notice further acknowledged that Defendant's investigations revealed that the compromised systems contained Plaintiff and Class Members' names, addresses, Social Security numbers, and driver's license or state identification numbers.

49. On or about April 11, 2022, Defendant disclosed the Data Breach to the Office of the Attorney General of Texas ("OAG"), indicating that it had identified at least 5,027 Texans whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

50. The fact that Defendant had to notify the OAG signifies that the accessed and stolen data was not encrypted or that the threat actor had the key required to decrypt the data.

51. To date, Defendant has not revealed the mechanism by which the unauthorized actor gained access to Defendant's IT environment and network.

52. Although Defendant acknowledged that it implemented additional security measures to further harden its digital environment, it has not disclosed what those security measures consist of.

53. Defendant's investigation could not rule out that information at issue has been or will be misused by the hackers.

54. This information was sensitive enough to materially increase the Plaintiff and Class Members' risk of identity theft and fraud, as demonstrated by Defendant's recommendation that Plaintiff and Class Members take significant actions and precautions to protect themselves from identity fraud and theft, including "remain[ing] vigilant by reviewing your account statements and credit reports closely," obtaining copies of annual credit reports, placing fraud alerts on credit reports, and placing a security freeze on credit files.

55. Plaintiff's and Class Members' PII was accessed and exfiltrated in the Data Breach.

56. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, because that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

57. Defendant acknowledged that it was compelled to enhance its then-existing cybersecurity measures thereby casting further doubt on Defendant's intrusion prevention and detection procedures and its system-monitoring controls.

58. Under Texas law, Defendant was required to disclose the breach of system security "without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred," except as provided by Tex. Bus. & Com. Code Ann. § 521.053.

59. As stated *supra*, it took Defendant nearly *seven months* to disclose the Data Breach to Plaintiff and Class Members.

60. During this time, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

D. Plaintiff Tarrant's Experience

61. Plaintiff Tarrant is a former Southland employee who began working at Southland as a machine operator around 2018. He left employment with Southland in early 2020 after suffering a work-related injury.

62. In exchange for his employment services, Defendant offered to compensate Plaintiff Tarrant and provide him with other employment benefits. To receive compensation and employment benefits, Defendant required Plaintiff Tarrant to: (i) provide Defendant with PII to fulfill Southland's legal responsibilities and operational requirements, including his full name, home address, Social Security Number, as well as PII of people designated as beneficiaries on his employment-related benefits through Defendant; and (iii) provide other confidential information as necessary.

63. Plaintiff Tarrant believes that this was a standard employment agreement and practice that Defendant had with its employees during his tenure at Southland.

64. Plaintiff Tarrant accepted Defendant's employment offer and provided the PII Southland required, expecting that Defendant would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed compensation and other employment benefits.

65. When he ended his employment with Defendant, Plaintiff Tarrant expected that Southland would continue to safeguard or destroy or archive his information securely.

66. Plaintiff Tarrant monitors his credit score using services like Credit Karma.

67. Around November 2021, Plaintiff Tarrant began receiving phone calls from numerous lenders both offering him loans and attempting to finalize loan applications submitted using his PII. Plaintiff Tarrant spent numerous hours calling and speaking with bank representatives to cancel the unauthorized loan applications and investigating their source.

68. As a result of the Data Breach, Plaintiff Tarrant suffered economic hardships and began soliciting lenders for credit to help meet his rental payments obligation and avoid eviction. The banks, however, kept denying him the credit he needed to stay afloat and after further investigation on his own he discovered that he was flagged due to credit misuse and that, as a direct and proximate result of the Data Breach and his PII being stolen, his credit score had tanked.

69. At this time, Plaintiff Tarrant became aware of several unauthorized attempts to obtain an extension of credit in his name without his consent on his credit report.

70. Around April 8, 2022, Plaintiff Tarrant received the Notice, first learned about the Data Breach, and realized that he was not only a victim of the Data Breach but that his PII was being used to commit identity theft and/or fraud.

71. Ultimately, Plaintiff Tarrant was unable to obtain credit and he was evicted from his home.

72. Plaintiff had a legally recognizable interest in preventing others from knowing, discovering, or disclosing sensitive confidential information pertaining to his private life.

73. Plaintiff Tarrant has suffered substantial, irreparable harm because his PII was compromised, disclosed, and/or misused by one or more criminals whose identity remains unknown. Tarrant's PII will remain in the public domain *indefinitely* and he must now deal with the overwhelming and constant fear and anxiety of further unauthorized misuse and exploitation of his confidential personal information for identity theft and fraud, and the humiliation caused by his status as a victim of identity theft/fraud and the feeling that other people will regard him with aversion or dislike.

74. As a result of Defendant's wrongful conduct, Plaintiff has spent and will spend time and money closely monitoring his identity and credit.

75. Indeed, Defendant's own Notice directs Plaintiff to spend time taking numerous steps to mitigate his damages, including, reviewing his account statements, notifying law enforcement, obtaining a copy of his credit report, placing a fraud alert on his accounts, putting a security freeze on his credit file, and contacting state and federal agencies about the Breach. This is time Plaintiff will never get back.

76. As a result of Defendant's wrongful conduct, Plaintiff Tarrant has been required to act in the protection of his interests by bringing this action against Defendant and is entitled to recover reasonable compensation for loss of time, attorney fees and other expenditures thereby suffered or incurred.

77. Plaintiff Tarrant is entitled to recover damages for all harm suffered—past, present, and future—legally caused by Defendant's wrongful conduct.

E. The Value of Personally Identifiable Information

78. Defendant knew or should have known that by collecting and storing Class Members' PII, it undertook a responsibility to take reasonable security measures to protect the

information from unlawful use, access, transfer or disclosure by unauthorized persons—that is, to protect the employees from the risk of identity theft and fraud.

79. In 2007, the United States Government Accountability Office released a report on data breaches (“GAO Report”) where it explained that “[t]he term ‘identity theft’ is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else’s name.”³

80. In today’s society, PII is a commodity. PII is an extremely valuable property right.⁴ Information compromised in data breaches can be used in a variety of unlawful manners. Moreover, non-PII can easily become PII when combined with additional information gathered from other sources.

81. One of the main reasons criminals steal PII is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims’ identities to engage in illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle, the more authentic pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a “social engineering” hacking technique to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number.

³ See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), <https://www.gao.gov/new.items/d07737.pdf> (last visited Nov. 3, 2021).

⁴ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted). Available at: <https://scholarship.richmond.edu/jolt/vol15/iss4/2>.

82. According to the Infosec Institute, sensitive personal information can sell for as much as \$363 per record in the black market. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.⁵

83. Unlike medical and health insurance information, Social Security numbers are such a significant identifier that they facilitate access by others to many of our most personal and private records and can enable someone to impersonate us to our embarrassment or financial loss.

84. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utility fraud, and bank/finance fraud.

85. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.⁶ Such fraud may go undetected until debt collection calls commence months, or even years, later.

86. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name. They may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. Each of these fraudulent activities is difficult to detect. An individual

⁵ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Nov. 3, 2021).

⁶ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 3, 2021).

may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

87. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as “[t]he credits bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”⁷

88. The PII targeted, compromised, accessed, and stolen in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

89. The information compromised in the Data Breach is impossible to “close” and difficult, if not impossible, to change: one's Social Security number.

90. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”

91. Defendant knew or should have known that unencrypted sensitive personal information amassed in computer systems lacking reasonably adequate cybersecurity measures,

⁷ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Nov. 3, 2021).

such as Defendant's, is valuable and highly sought after by nefarious third parties seeking to unlawfully monetize that information.

92. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant economic and noneconomic harms that Plaintiff and Class Members would suffer as a consequence.

93. Additionally, the risk of harm to Plaintiff and Class Members from Defendant's failure to take precautionary measures was readily and clearly foreseeable.

94. It is a matter of common knowledge in Defendant's industry that businesses like Defendant's face a higher threat of security breaches due in part to the large amounts of data and PII they possess.

95. Experts studying cybersecurity routinely identify business like Defendant's as particularly vulnerable to cyberattacks because they sit on a gold mine of value PII, they often have lesser IT defenses and a high incentive to quickly regain access to their data.

96. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed.

97. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

records, May 2020), NMSI knew or should have known that its electronic records would be targeted by cybercriminals.

98. Defendant knew or should have known its security systems were inadequate, particularly in light of the prior data breaches experienced by similar companies, and yet Defendant failed to take reasonable precautions to safeguard Plaintiff's and Class Members' PII.

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

F. Laws and Industry Customs and Standards Underscore Defendant's Duty to Implement Reasonable Information Security Practice.

100. While cybersecurity risks cannot be eliminated, they can be reasonably detected, prevented, and mitigated through cybersecurity standards, guidelines, and best practices.

101. Defendant could have prevented the Data Breach by implementing administrative, technical, and physical safeguards appropriate to Defendant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about employees.

102. Defendant could have implemented these safeguards without undue burden, such as properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members, taking complete inventory of the sensitive information in its possession or control, and requiring multifactor authentication from users attempting to access its information system.

103. Multifactor authentication is a basic security feature that deters and prevents cyberattacks by requiring that users present two or more pieces of information, usually (i) a password and (ii) a one-time code, before users are granted access. It is so simple, effective, and

inexpensive that even free services like Gmail and Facebook offer it and encourage people to use it.

104. Defendant's failure to encrypt Plaintiff and Class Members' sensitive information and implement minimum and basic cybersecurity precautions that a reasonable and prudent business would under similar circumstances constitutes a reckless disregard for Plaintiff and Class Members' privacy rights and rises to the level of gross negligence.

105. Under Tex. Bus. & Com. Code Ann. § 521.002, the term "Sensitive Personal Information" means:

- (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
 - (i) social security number;
 - (ii) driver's license number or government-issued identification number; or
 - (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- (B) information that identifies an individual and relates to:
 - (i) the physical or mental health or condition of the individual;
 - (ii) the provision of health care to the individual; or
 - (iii) payment for the provision of health care to the individual.

Tex. Bus. & Com. Code Ann. § 521.002.

106. An entity doing business in Texas must "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business." Tex. Bus. & Com. Code § 521.052. Business Duty to Protect Sensitive Personal Information

107. An entity doing business in Texas must "destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business." Tex. Bus. & Com. Code § 521.052. Business Duty to Protect Sensitive Personal Information.

108. In addition, the duty to employ reasonable security measures is highlighted under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data and misrepresenting their information collection practices contained within privacy policies.

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

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

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

112. The FTC has brought enforcement actions against businesses for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

113. Lastly, security standards apply to businesses like Defendant's that protect PII. For example, the Computer Security Division of the National Institute of Standards and Technology's (NIST) Information Technology Laboratory provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services. Also, the PCI Security Standards Council provides standards and supporting materials to enhance payment card data security.

114. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound emails using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed, and

those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with the least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

115. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization’s helpdesk, search the internet for the sender organization’s website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)
....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website’s security to ensure the information you submit is encrypted before you provide it...
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic...⁸

116. To prevent and detect cyber-attacks attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as a potential full compromise;

Include IT Pros in security discussions

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

Build credential hygiene

⁸ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Nov. 11, 2021).

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

Apply the principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁹

G. Plaintiff and Class Members Have and Will Continue to Be Harmed as a Consequence of Defendant's Information Security Failures and Tortious Conduct.

117. Juxtaposed against the basic and inexpensive security measures Defendant was required to implement are the immediate, substantial, and long-lasting harms that Plaintiff and Class Members will suffer due to Defendant's conduct.

118. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

119. When individuals have their PII stolen, they are at risk for identity theft, and need to: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain

⁹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

120. Data breach victims must spend significant time indefinitely monitoring their financial accounts. It must be noted that generally, there is a significant gap between the time the initial data breach occurs and when it is discovered, and also between the time when PII are stolen and when it is eventually used.

121. PII is such a valuable commodity to identity thieves that criminals often trade the information on the “cyber black-market” for years once the information has been compromised.

122. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data might 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.

See GAO Report, at p. 29.

123. The GAO observed that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”¹⁰

¹⁰ *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), <https://www.gao.gov/new.items/d07737.pdf> (last visited Nov. 3, 2021).

124. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹¹

125. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

126. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

127. Therefore, the complimentary fraud and identity monitoring service offered by Defendant is wholly inadequate as the benefits are only provided for 12 months, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

128. As one commentator explained, “While helpful in detecting identity theft attempts following the breach, credit monitoring is far from a complete solution for several reasons. These reasons include the fact that credit monitoring has limited ability, detecting only credit fraud, and not detecting other types of fraud such as filing a false tax return. Also, credit monitoring is offered for a limited time. Fraudulent use of the stolen credit information often occurs after the credit monitoring ends.”

¹¹ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited Nov. 3, 2021).

129. Plaintiff and Class Members retain a significant interest in ensuring that their PII, which remains in Defendant's possession, is protected from further exposure and in being awarded damages compensate for all the relevant injuries, past and future.

130. On information and belief, Defendant has still not implemented critical computer systems and data security practices to ensure that affected individuals' PII will not be accessed or stolen by other cyber criminals. The remediation measures implemented by Defendant and its Affiliates provided only an immediate stop to the present attack.

131. Defendant must put into place a security management framework, as defined by numerous government standards, and conduct audits by third-party independent auditors regularly to ensure that it keeps abreast of future threats to the PII in its care.

CLASS ACTION ALLEGATIONS

132. Plaintiff incorporates by reference all other paragraphs of this Petition as if fully set forth herein.

133. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Tex. R. Civ. P. 42.

134. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seek certification of the following Class:

All persons Southland identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach on or about April 8, 2022.

135. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, their staffs, as well as their immediate family members.

136. Plaintiff reserves the right to amend the definitions of the Class or add a class or subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

137. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

138. This action satisfies the requirements for a class action under Tex. R. Civ. P. 42, including requirements of numerosity, commonality, typicality, and adequacy of representation.

139. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, reports indicate that thousands of individuals had their PII compromised in the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

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

- Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant owed a duty to Class Members to safeguard their PII;
- Whether Defendant breached its duty to Class Members to safeguard their PII;
- Whether unauthorized third parties obtained Class Members' PII in the Data Breach;
- Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- Whether Defendant's conduct was negligent;
- Whether Defendant's conduct was grossly negligent;
- Whether Defendant's conduct was per se negligent, and;
- Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

141. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

142. **Fair and Adequate Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

143. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

145. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

146. Likewise, the issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a) Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- b) Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- c) Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

- d) Whether Defendant failed to take commercially reasonable steps to safeguard employee PII; and
- e) Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

147. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

Count I: Negligence

(On Behalf of Plaintiff and the Class)

148. Plaintiff realleges and incorporates by reference in this count all paragraphs above as if fully set forth herein and further alleges:

149. Defendant required Plaintiff and the members of the Class to submit sensitive non-public PII as a condition of their employment or a condition for applying for employment.

150. Defendant encouraged Plaintiff and the members of the Class to rely on its information security practices.

151. Plaintiff and Class Members had a reasonable expectation of privacy in the PII disclosed to Defendant.

152. As an employer, Defendant is in a special relationship with Plaintiff and Class Members, which includes the duty to protect them against unreasonable risks of harm and negligent and intentional misconduct.

153. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices.

154. The risk and probability of harm to the Plaintiff and Class Members from Defendant's failure to take precautionary measures was readily and clearly foreseeable. Not only was Defendant aware of the risk created by its inaction, but it was also in a unique position to know of the risk and prevent it.

155. Defendant knew or should have known that it was a high-value target at a heightened risk of security breaches.

156. The breach of security was reasonably foreseeable given the high frequency of cyberattacks and data breaches in Defendant's industry.

157. It was therefore foreseeable that the failure to adequately safeguard Class Members' sensitive PII would result in one or more types of injuries to Class Members.

158. Defendant's conduct was unreasonable in light of the recognizable risk of injury.

159. Defendant failed to exercise that degree of care that would be used by a person or company of ordinary prudence under the same or similar circumstances.

160. Defendant failed to implement and maintain reasonable procedures to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

161. Defendant failed to destroy or arrange for the destruction of consumer and employee records containing sensitive PII within the business's custody or control that were no longer needed.

162. Defendant misrepresented its information collection, maintenance, and destruction practices.

163. Defendant failed to timely notify affected individuals about the Data Breach.

164. Defendant's own conduct created or exposed Plaintiff and Class Members to a recognizable high degree of risk of harm through its misconduct.

165. Defendant's conduct involved a high degree of probability that it would defeat the measures Plaintiff and Class Members had taken to maintain the privacy and confidentiality of their PII.

166. Defendant knew or should have known that its cybersecurity measures were inadequate and in need of upgrading, yet it failed to take appropriate corrective measures.

167. Defendant was in possession or control of property that afforded a peculiar temptation or opportunity for intentional interference with Plaintiff's and Class Members' legally protected interests that was likely to cause them harm.

168. Defendant acted with knowledge of peculiar conditions that created a high degree of risk of intentional misconduct, e.g., Defendant was aware of inadequacy of its cybersecurity.

169. Defendant failed to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

170. Defendant failed to identify foreseeable threats and vulnerabilities that could impact PII.

171. Defendant failed to implement reasonable security measures designed to prevent this type of attack even though there have been similar attacks on similar businesses.

172. Additional negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement and maintain adequate security measures to safeguard Class Members' PII;

- Failing to adequately monitor the security of its networks and systems;
- Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;
- Allowing unauthorized access to Class Members' PII;
- Failing to detect in a timely manner that Class Members' PII had been compromised;
- Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

173. The tortious conduct described above was a substantial factor in bringing about the Data Breach, and without which conduct such breach of security would not have occurred.

174. The unauthorized access, theft, exfiltration, and misuse of Plaintiff and Class Members' sensitive PII is a foreseeable result and natural consequence of Defendant's tortious conduct.

175. A business using ordinary care would have foreseen that the Data Breach, or some similar event, might reasonably result from the tortious conduct described above.

176. Reasonable and adequate security measures could have prevented the Data Breach.

177. But for Defendant's failure to implement and maintain adequate security measures to protect its employees' PII and failure to monitor its systems to identify suspicious activity, the PII of Plaintiff and Class Members would not have been stolen, Plaintiff and Class Members would not have been injured, and Plaintiff and Class Members would not be at a heightened risk of identity theft in the future.

178. Defendant's negligence was a substantial factor in causing harm to Plaintiff and Class Members. As a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, the PII of Defendant's employees was accessed by unauthorized individuals who: (i) have already used the compromised information to commit identity theft and fraud; (ii) can continue to use this compromised PII to commit identity theft and identity and health care and/or medical fraud; and (iii) have posted the information on the internet, allowing themselves and others to commit identity theft, and identity and health care and/ or medical fraud using the compromised PII indefinitely.

179. Defendant's conduct involved an extreme degree of risk, considering the probability and magnitude of the potential harm to Plaintiff and Class Members.

180. Defendant had actual, subjective awareness of the risk involved, but nevertheless proceeded with conscious indifference to the rights, safety, or welfare of Plaintiff and Class Members.

181. The injuries suffered by Plaintiff and Class Members are a natural and foreseeable consequence of Southland's failure to employ reasonable security protections of its employees PII.

182. As a result, Plaintiff and other impacted individuals suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

Count II: Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

183. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

184. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of employment and/or use of Defendant's services.

185. Plaintiff and Class Members disclosed their PII in exchange for services and/or employment, along with Defendant's promise to protect their PII from unauthorized disclosure.

186. On information and belief, in its written privacy policies, Defendant expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

187. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

188. There was a meeting of the minds and an implied contractual agreement between Plaintiff and Class Members and the Defendant, under which Plaintiff and Class Members would provide their PII in exchange for Defendant's obligations to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

189. When Plaintiff and Class Members provided their PII to Defendant as a condition of obtaining employment they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

190. Defendant solicited, invited, and then required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

191. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

192. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

193. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

194. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

195. As a direct and proximate result of Defendant breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

197. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Count III: Negligence Per Se
(On Behalf of Plaintiff and the Class)

198. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

199. Section 5 of the FTC Act, 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 Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

200. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

201. Defendant’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

202. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

203. As a direct and proximate result of Defendant’s negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the

compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count IV: Unjust Enrichment

(On Behalf of Plaintiff and the Class)

204. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

205. This claim is plead in the alternative to the Second Cause of Action for breach of implied contract.

206. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

207. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

208. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of labor services, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

209. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

210. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

211. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

212. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

213. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

214. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

DAMAGES OR EQUITABLE REMEDIES

183. Defendant's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.

184. As a result of Defendant's negligence, Plaintiffs and members of the class have suffered and will suffer injury, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendant for the purpose of deriving employment from Defendant and with the

understanding that Defendant would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII which remains in Defendant's possession and are subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Class members.

JURY DEMAND

185. Plaintiff demands a trial by jury on all issues so triable, Plaintiff has tendered the jury fee via online payment concurrently herewith.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment against Southland as follows:

- For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;
- For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to employee data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;
- For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- For an award of punitive damages, as allowable by law;
- For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- Pre- and post-judgment interest on any amounts awarded and
- Such other and further relief as this court may deem just and proper.

Dated: May 20, 2022

Respectfully submitted,

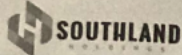


William B. Federman
TX Bar No. 00794935
FEDERMAN & SHERWOOD
212 W. Spring Valley Road,
Richardson, Texas 75081
AND
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Phone: (405) 235-1560
Fax: (405) 239-2112
wbf@federmanlaw.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

**Pro hac vice forthcoming*

EXHIBIT A



P.O. Box 989728
West Sacramento, CA 95798-9728



To Enroll, Please Call:

1-833-774-2186

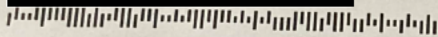
Or Visit:

<https://response.idx.us/SouthlandEnrollment>

Enrollment Code: T7FYLL88EV



Dennis Tarrant



April 8, 2022

Notice of Data Security Incident

Dear Dennis Tarrant,

We are writing to inform you of a data security incident experienced by Southland Holdings LLC ("Southland") that may have involved your personal information. Please read carefully, as this letter contains background information about the incident, the type of information involved, and steps you can take to protect your personal information.

What Happened: On September 21, 2021, Southland discovered potential unauthorized access to our environment. Upon discovery, we took immediate steps to secure our systems prior to restoration. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident. Based on the findings from the investigation, we reviewed the affected systems to determine whether personal information was impacted as a result of the incident. Once it was confirmed that data containing personal information was potentially accessed as a result of the incident, an in-depth and thorough review of the data was undertaken to identify the individuals to whom the information pertained. On February 11, 2022, we determined that the affected systems contained some of your personal information.

What Information Was Involved: The information involved may have included your name, address, Social Security number, and driver's license or state identification number.

What We Are Doing: As soon as we learned of the incident, we immediately began containment, mitigation, and restoration efforts. We also launched an investigation and engaged outside cybersecurity experts to assist us in determining what happened. As part of the response processes, we implemented additional security measures to further harden our digital environment in an effort to prevent a similar event from occurring in the future. In addition, we reported the incident to the Federal Bureau of Investigation and are committed to providing the FBI and law enforcement whatever assistance is needed.

Furthermore, even though there is no evidence of misuse of information involved in this incident, we are providing you with information about steps that you can take to help protect your personal information. Additionally, as an added precaution, we are offering you 12 months of identity theft protection services through IDX, a data breach and recovery services expert. These identity protection services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

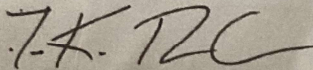
What You Can Do: We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-774-2186 or going to <https://response.idx.us/SouthlandEnrollment> and using the Enrollment Code provided above. Representatives are available between 8:00am and 8:00pm Central Time from Monday to Friday.

Please note that the deadline to enroll is July 8, 2022. In addition, you can review the resources provided on the following pages for additional steps to protect your personal information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the credit and identity monitoring services, please call 1-833-774-2186 or go to <https://response.idx.us/Southland> Enrollment between 8:00am and 8:00pm Central Time.

The security of your information is a top priority for Southland, and we are committed to safeguarding your data and privacy. Please accept our sincere apologies and know we deeply regret any concern or inconvenience this may cause you.

Sincerely,



Frank Renda
Chief Executive Officer
Southland Holdings LLC

Steps You Can Take to Protect Your Personal Information



007295

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

**Washington D.C. Attorney
General**
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete