IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

LANDON JOHNSON, individually and on behalf of all similarly situated persons, Plaintiff, v. O.K. FOODS, INC. Defendant.	Case No. CIV-21-561-J **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Landon Johnson ("Mr. Johnson" or "Plaintiff Johnson"), individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant O.K. Foods, Inc. ("OK Foods"), and alleges as follows:

INTRODUCTION

1. Part of the bargain of obtaining a job requires turning over to employers valuable personal identifying information ("PII"),[1] including names, Social Security numbers, birthdates and addresses. Identity thieves can use this highly sensitive

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in myriad schemes, all of which can cause grievous financial harm, negatively impact the victim's credit scores for years, and cause victims to spend countless hours mitigating the impact.

2. Every year millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers' and employees' data.

3. OK Foods, one of the world's largest fully-integrated chicken producers, is among those companies which have failed to meet their obligation to protect the sensitive PII entrusted to them by their current and former employees.

4. As reported by OK Foods, between April 22, 2020 and April 30, 2020, an unknown third party gained unauthorized access to an OK Foods employee email address that contained certain highly sensitive and unencrypted employee data. Employee names and Social Security numbers were among the PII accessed and obtained by the unauthorized party.

5. Defendant OK Foods required its employees to provide it with their sensitive PII. Defendant had an obligation to secure that PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiff and

Class[2] Members and OK Foods.

6. As a result of OK Foods' failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiff and the Class are now at much higher risk of identity theft and of cybercrimes of all kinds, especially considering the highly sensitive PII stolen here.

THE PARTIES

7. Defendant O.K. Foods, Inc., is an Arkansas corporation with numerous hatcheries, farms, feed mills, and processing plants across the country. Its corporate headquarters are located in Fort Smith, Arkansas.

8. OK Foods is wholly owned by Bachoco USA, LLC, a Delaware corporation. Bachaco USA, LLC is a wholly owned subsidiary of Industrias Bachoco S.A. de C.V., a publicly held corporation headquartered in Guanajuato, Mexico.

9. OK Foods has evolved from a livestock and poultry feed manufacturer to one of the world's largest fully integrated chicken producers, with over three thousand five hundred (3,500) employees providing chicken products to people around the globe.

10. Plaintiff Johnson is a resident of Sequoyah County, Oklahoma and was employed by OK Foods in Muldrow, Oklahoma in or about September 2016.

[2] As used herein, the terms "Class" or "Class Members" means the putative Nationwide Class and Oklahoma Subclass defined below.

11. Mr. Johnson reasonably believed OK Foods would keep his PII secure. Had OK Foods disclosed to him that his PII would not be kept secure and would be easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII.

JURISDICTION AND VENUE

12. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

13. This Court has personal jurisdiction over Defendant because it is registered to conduct business in Oklahoma and has sufficient minimum contacts with Oklahoma.

14. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of its business in this District and Defendant has caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

A. OK Foods collects and stores thousands of current and former employees' PII and failed to provide adequate data security to protect it.

15. OK Foods, which is headquartered in Arkansas with locations in Oklahoma, was founded more than eighty (80) years ago and has evolved from a livestock and poultry feed manufacturer to one of the world's largest fully integrated chicken producers.

16. Currently OK Foods, a publicly traded company, employs over three thousand five hundred (3,500) employees, has tens of thousands of former employees, and

is a major player in its industry. In addition to operating hatcheries, farms, feed mills, and processing plants across the country, OK Foods prides itself on "nourishing [its] consumers, [its] employees, our environment, and [its] shareholders."[3] OK Foods also touts on its website its company values of honesty, responsibility, respect, service, and justice.[4]

17. OK Foods claims it "understands the importance of protecting the security of [] Personal Info."[5] Moreover, OK Foods promises that "all Personal Info is encrypted and stored on secured servers."

B. OK Foods' inadequate data security exposed its current and former employees' sensitive PII.

18. Between April 22, 2020 and April 30, 2020, an unknown third party gained access to an OK Foods' employee's email account where highly sensitive employee data was being contained, unencrypted.

19. Between April 22, 2020 and April 30, 2020, unauthorized, unknown third party cyber criminals accessed OK Foods' employees' PII, which included names and Social Security numbers.

20. This incident is referred to herein as the "Data Breach."

21. Plaintiff received a letter from OK Foods dated April 15, 2021 (the "Notice Letter," attached hereto as **Exhibit 1**), almost a full year since the Data breach occurred. The Notice Letter stated that his PII may have been compromised, and included the following:

[3] https://www.okfoods.com/about-us/ (last accessed June 1, 2021).
[4] *Id.*
[5] https://www.okfoods.com/privacy-policy (last accessed June 1, 2021).

What Happened?

As a result of a phishing incident, an unauthorized party obtained access to an OK Foods employee's email account.

What Are We Doing?

Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, we determined on March 18, 2021 that the impacted email account, which was accessed between April 22, 2020 and April 30, 2020, contained some of your personal information. We have no evidence that your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

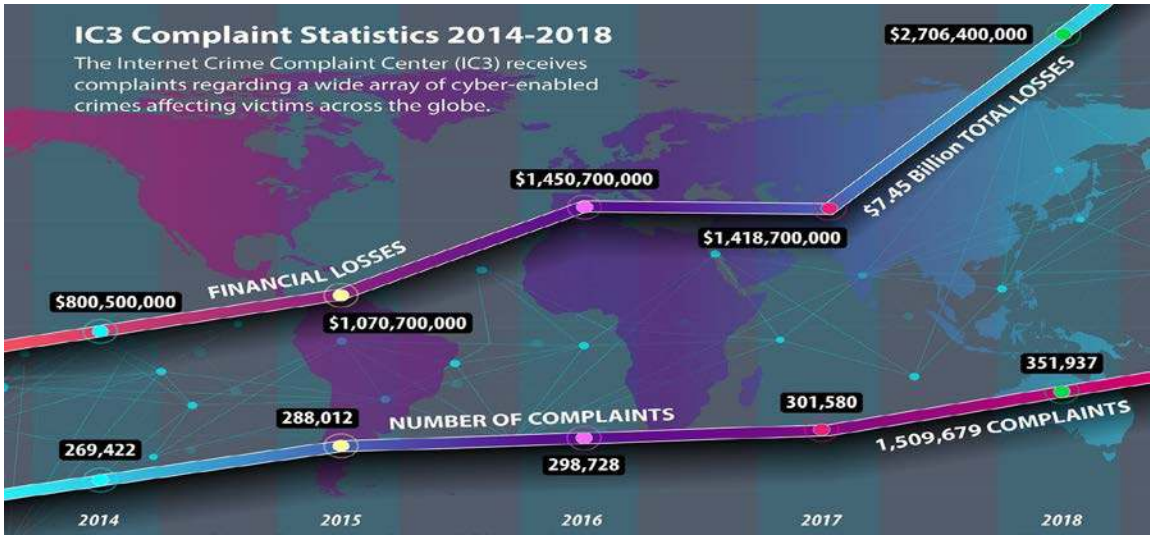
The email account that was accessed contained some of your personal information, specifically your full name and Social Security number.

22. After receiving the Notice Letter, it is reasonable for recipients, including Plaintiff and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, in OK Foods' letter, it warns affected individuals of the "potential misuse of your information," and that impacted individuals should, among other things, "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis." *See* **Exhibit 1**.

C. The PII exposed by OK Foods as a result of its inadequate data security is highly valuable on the black market.

23. The information exposed by OK Foods is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

24. This exposure is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



25. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[6]

26. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

27. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[7]

---

[6] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[7] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed June 1, 2021).

28. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[8]

29. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[9]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[10]. Criminals can also purchase access to entire company data breaches from $900 to $4,500[11].

---

[8] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed June 1, 2021).

[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 accessed June 1, 2021).

[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 accessed June 1, 2021).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 1,

30. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems[12].

31. What is more, it is no 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. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

32. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

2021).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 1, 2021).

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*,

33. Because of this, the information compromised in the Data Breach here is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

34. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[14]

35. Once PII is sold, it is often used 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.

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

NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 1, 2021).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 1, 2021).

37. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and Class Members that their PII had been stolen. It took Defendant almost a year to determine the information had been compromised. Plaintiff was not notified until a year *after* the impacted email account containing the PII had been accessed.

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

39. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

40. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[15] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and 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 damage

[15] *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), https://www.gao.gov/assets/gao-07-737.pdf (last visited June 1, 2021).

to their credit records . . . [and their] good name."[16]

D. OK Foods Failed to Comply with Federal Trade Commission Requirements.

41. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

42. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[18] Among other things, the guidelines note businesses should 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 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

---

[16] *Id.*
[17] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 1, 2021).
[18] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 1, 2021).

event of a breach.[19]

43. Additionally, the FTC recommends that companies 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.[20]

44. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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 Federal Trade Commission Act ("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.[21]

45. By being negligent in securing Plaintiff's and Class Members' PII and allowing an unknown third party to access an OK Foods employee's email account in order to access unencrypted employee PII, OK Foods failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. OK Foods' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[19] *Id.*
[20] Federal Trade Commission, *Start With Security*, *supra footnote 17*.
[21] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 1, 2021).

E. Plaintiff Johnson's Experience

46. Plaintiff Johnson was employed by OK Foods in or about September 2016 in Muldrow, Oklahoma.

47. On or around April 15, 2021, Plaintiff Johnson received the Notice Letter from OK Foods informing him of the Data Breach.

48. After receiving notification of the Data Breach, Plaintiff Johnson noticed a dramatic uptick in the amount and frequency of phishing emails he was receiving.

49. As a result of the Data Breach, Plaintiff Johnson has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through his unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

50. Plaintiff Johnson is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

51. Plaintiff Johnson stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the few online accounts that he has.

52. Plaintiff Johnson has suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Johnson entrusted to Defendant for the purpose of his employment. This PII was compromised in, and has been diminished as a result of, the Data Breach.

53. Plaintiff Johnson has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

54. Plaintiff Johnson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his full name, which PII is now in the hands of cyber criminals and other unauthorized third parties.

55. Knowing that thieves stole his PII, including his Social Security Number and potentially his driver's license number and other PII that he was required to provide to OK Foods, and knowing that his PII will be sold on the dark web, has caused Plaintiff Johnson great anxiety.

56. Additionally, Plaintiff Johnson has not been involved in any data breaches and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

57. Plaintiff Johnson has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

58. As a result of the Data Breach, Plaintiff Johnson will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

F. Plaintiff and the Class Members suffered damages.

59. The ramifications of Defendant's failure to keep current and former employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[22]

60. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

61. Defendant required Plaintiff and Class Members to provide their PII, including full names and Social Security numbers. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

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

---

[22] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed June 1, 2021).

63. The Data Breach was a direct and proximate result of OK Foods' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

64. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former employees' PII, and despite its public statements that OK Foods "understands the importance of protecting the security of [] Personal Info" and OK Foods' promise that "all Personal Info is encrypted and stored on secured servers."

65. Had Defendant remedied the deficiencies in its data security training and protocols, and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

66. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

67. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[23]

68. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts 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 theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

[23] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed June 1, 2021).

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

69. In addition to a remedy for the economic harm, Plaintiff and the Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

70. To date, other than providing a woefully inadequate twelve (12) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiff and Class Members other than simply telling them to review their financial records and credit reports on a regular basis.

71. This type of recommendation, however, does not require Defendant to expend any effort to protect Plaintiff's and Class Members' PII.

72. Defendant's failure to adequately protect Plaintiff's and Class Members' PII has resulted in Plaintiff and Class Members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's Notice Letter indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

73. Defendant's offer of 12 months of identity monitoring and identity protection services to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is

used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[24] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection. Although their PII was improperly exposed in or about April 2020, affected current and former employees were not notified of the Data Breach until a year later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of OK Foods' delay in detecting and notifying current and former employees of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

74. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and the following proposed Nationwide Class, defined as follows:

> All persons residing in the United States who are current or former employees of OK Foods or any OK Foods affiliate, parent, or subsidiary, and had their PII compromised as a result of the Data Breach that occurred between April 22, 2020 and April 30, 2020.

In addition, Plaintiff brings this action on behalf of himself and the following proposed Oklahoma Subclass defined as follows:

> All persons residing in the State of Oklahoma who are current or former employees of OK Foods or any OK Foods affiliate, parent, or

[24] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited June 1, 2021).

subsidiary, and had their PII compromised as a result of the Data Breach that occurred between April 22, 2020 and April 30, 2020.

75. Both the proposed Nationwide Class and the proposed Oklahoma Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

76. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of OK Foods; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

77. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

78. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PII in violation Section 5 of the FTC Act;

g. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

79. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

80. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

81. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

82. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Oklahoma Subclass)

83. Plaintiff incorporates the foregoing paragraphs as though fully set forth

herein.

84. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected.

85. Defendant owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former employees.

86. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former employees and exchanging it through email correspondence, and the critical importance of adequately securing such information.

87. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard it, that Defendant would not store it longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

88. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Defendant's misconduct included failing to implement the necessary systems, policies, employee training and procedures necessary to prevent the

Data breach.

89. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

90. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

91. Plaintiff's injuries and damages, as described below, are a reasonably certain consequence of OK Foods' breach of its duties.

92. Because Defendant knew that a breach of its systems would damage thousands of current and former OK Foods employees whose PII was inexplicably contained, unencrypted, in email accounts, Defendant had a duty to adequately protect its data systems and the PII contained therein.

93. Defendant had a special relationship with current and former employees, including with Plaintiff and Class Members, by virtue of their being current or former employees. Plaintiff and Class Members reasonably believed that Defendant would take adequate security precautions to protect their PII. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII.

94. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from

being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class Members during the time it was within Defendant's possession or control.

95. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access an OK Foods' employee's email account containing the PII at issue, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

96. Defendant's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

97. Neither Plaintiff nor the other Class Members contributed to the Data Breach as described in this Complaint.

98. As a direct and proximate cause of Defendant's actions and inactions, including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiff and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort

expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and (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.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff, the Nationwide Class or, alternatively, the Oklahoma Subclass)

99. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

100. Defendant offered employment to the current or former employees, including Plaintiff and Class Members, either directly or through acquiring the businesses for which Plaintiff and Class Members worked, in exchange for compensation and other employment benefits.

101. Defendant either required Plaintiff and Class Members to provide their PII, or acquired their PII from their former employers, including names, addresses, dates of

birth, Social Security numbers, driver's license numbers, passport numbers and other personal information. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

102. These exchanges constituted an agreement between the parties: Plaintiff and Class Members would provide their PII in exchange for the prospect of employment and benefits provided by Defendant.

103. These agreements were made either by Plaintiff or Class Members applying for employment with Defendant, being employed by Defendant, or their employers being acquired by Defendant.

104. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members compensation and other employment benefits, or, in the case of applicants, consider hiring them.

105. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure and/or use.

106. Plaintiff and Class Members accepted Defendant's employment offer and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

107. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendant.

108. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' PII.

109. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class Members violated the purpose of the agreement between the parties: Plaintiff's and Class Members' employment in exchange for compensation and benefits.

110. Defendant was on notice that its systems and data security protocols could be inadequate yet failed to invest in the proper safeguarding of Plaintiff's and Class Members' PII.

111. Instead of spending adequate financial resources to safeguard Plaintiff's and Class Members' PII, which Plaintiff and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class Members.

112. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

THIRD CAUSE OF ACTION
Breach of Confidence
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Oklahoma Subclass)

113. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

114. At all times during Plaintiff's and Class Members' interactions with Defendant as its employees, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

115. Plaintiff's and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

116. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

117. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

118. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

119. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices and providing proper employee training to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

120. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

121. But for Defendant's disclosure of Plaintiff's and Class Members' PII through its employee's email account, in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

122. This disclosure of Plaintiff's and Class Members' PII constituted a violation of Plaintiff's and Class Members' understanding that Defendant would safeguard and protect the confidential and novel PII that Plaintiff and Class Members were required to disclose to Defendant.

123. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew its data security procedures for accepting and securing Plaintiff's and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' PII in jeopardy.

124. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and/or are at a substantial risk of suffering injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On behalf of Plaintiff and the Nationwide Class and Oklahoma Subclass)

125. Plaintiff incorporates the foregoing paragraphs as though fully set forth

herein.

126. Oklahoma establishes the right to privacy in the Oklahoma Constitution's Right to Privacy clause. *See* Okla. Const. Art. II, Section 30.

127. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

128. Defendant owed a duty to its employees, including Plaintiff and Class Members, to keep their PII confidential.

129. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the PII that is the subject of this action, is highly offensive to a reasonable person.

130. The intrusion was into a place or thing that was private and is entitled to remain private. Plaintiff and Class Members disclosed their PII to Defendant as part of their employment with Defendant, but did so privately with the intention and understanding that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendant's negligent actions and inactions, constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

132. Defendant invaded Plaintiff's and Class Members' privacy by failing to adequately implement data security measures, despite its obligations to protect current and former employees' highly sensitive PII.

133. Defendant's motives leading to the Data Breach were financially based. In order to save on operating costs, Defendant decided against the implement of adequate data security measures.

134. Defendant's intrusion upon Plaintiff's and Class Members' privacy in order to save money constitutes an egregious breach of social norms.

135. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

136. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

137. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

138. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class and Oklahoma Subclass)

139. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

140. In light of their special relationship, Defendant became the guardian of Plaintiff's and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its employees' PII, to act primarily for the benefit of those employees, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' PII and to timely detect and notify them in the event of a data breach.

141. In order to provide Plaintiff and Class Members compensation and employment benefits, or to consider Plaintiff and Class Members for employment, Defendant required that Plaintiff and Class Members provide their PII.

142. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class Members' PII for the benefit of Plaintiff and Class Members in order to provide Plaintiff and Class Members compensation and employment benefits.

143. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with them. Defendant breached

its fiduciary duties owed to Plaintiff and Class Members by failing to properly encrypt and otherwise protect Plaintiff's and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiff and Class Members of the Data Breach.

144. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (g) 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 Plaintiff and Class Members.

145. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury

and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Nationwide Classes and Oklahoma Subclass)

146. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

147. As described above, when Plaintiff and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiff's and Class Members' PII and to timely detect and notify them in the event of a data breach.

148. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide their PII in exchange for employment and benefits provided by Defendant.

149. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members compensation and other employment benefits.

150. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

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

152. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

153. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII; storing the PII former employees, despite any valid purpose for the storage thereof having ceased upon the termination of the employment relationship with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendant's data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

154. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

155. Likewise, all conditions required for Defendant's performance were met.

156. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

157. Plaintiff and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual

identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

158. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

159. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

SEVENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiff and Nationwide Classes and Oklahoma Subclass)

160. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

161. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

162. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

163. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure their PII.

164. Defendant still possesses PII regarding Plaintiff and Class Members.

165. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its

computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

166. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

167. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

168. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

169. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a

periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

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

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

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

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of himself and all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiff as Class Representative and the undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting OK Foods from engaging in the wrongful and unlawful acts described herein;

ii. requiring OK Foods to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring OK Foods to delete, destroy, and purge the PII of Plaintiff and Class Members unless OK Foods can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring OK Foods to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members' PII;

v. prohibiting OK Foods from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

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

vii. requiring OK Foods to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring OK Foods to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring OK Foods to segment data by, among other things, creating firewalls and access controls so that if one area of OK Foods' network is compromised, hackers cannot gain access to other portions of OK Foods' systems;

x. requiring OK Foods to conduct regular database scanning and securing checks;

xi. requiring OK Foods to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well

as protecting the PII of Plaintiff and Class Members,

xii. requiring OK Foods to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring OK Foods to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with OK Foods' policies, programs, and systems for protecting PII;

xiv. requiring OK Foods to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor OK Foods' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring OK Foods to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring OK Foods to implement logging and monitoring programs sufficient to track traffic to and from OK Foods' servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate OK Foods' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to detect and disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiff and Class Members damages;

f. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Date: June 2, 2021

Respectfully Submitted,

s/ William B. Federman
William B. Federman, OBA #2853
Tyler J. Bean, OBA #33834
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
tjb@federmanlaw.com

M. Anderson Berry
(Pro Hac Vice application forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Attorneys for Plaintiff and the Class

EXHIBIT 1

O
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

April 15, 2021

Landon Johnson H-12558
[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear Landon Johnson:

We are writing with important information regarding a recent data security incident. The privacy and security of the personal information we maintain is of the utmost importance to OK Foods. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

As a result of a phishing incident, an unauthorized party obtained access to an OK Foods employee's email account.

What We Are Doing.

Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, we determined on March 18, 2021 that the impacted email account, which was accessed between April 22, 2020 and April 30, 2020, contained some of your personal information. We have no evidence that your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The email account that was accessed contained some of your personal information, specifically your full name and Social Security number.

What You Can Do.

To protect you from any potential misuse of your information, and to demonstrate our commitment to the protection of your information, we are offering you a complimentary one-year membership of Experian's® IdentityWorks℠ at no cost to you. This product provides you with superior identity detection and resolution of identity theft. For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

Also provided in "Other Important Information" are other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **June 21, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code:** [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP.

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 1-877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

5. [illegible]

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
LANDON JOHNSON, individually and on behalf of all similarly situated persons,

(b) County of Residence of First Listed Plaintiff Sequoyah
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
William B. Federman & Tyler J. Bean, Federman & Sherwood
10205 N. Pennsylvania Ave., Oklahoma City, OK 73120
(405) 235-1560

DEFENDANTS
O.K. FOODS, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*
- ❒ 3 Federal Question *(U.S. Government Not a Party)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	❒ 4
Citizen of Another State	❒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	☒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. § 1332(d), Class Action Fairness Act

Brief description of cause:
Privacy Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):
JUDGE _____ DOCKET NUMBER _____

DATE
06/02/2021

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____