

**CAUSE NO: 067-348166-23**

|                                                                                                                                                                                                                                   |                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>JEREMY P. BACA, DYLAN LAMOREAUX, PETER SALINAS, and CURTIS LANE</b> on behalf of themselves and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br><b>BEN E. KEITH COMPANY,</b><br><br>Defendant. | IN THE DISTRICT COURT<br><br><br><br><br>TARRANT COUNTY, TEXAS<br><br><br><br><br>67 <sup>th</sup> JUDICIAL DISTRICT |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|

**PLAINTIFFS' FIRST AMENDED CLASS ACTION PETITION**

Plaintiffs Jeremy P. Baca, Dylan Lamoreaux, Peter Salinas, and Curtis Lane on behalf of themselves and on behalf of the Class defined below of similarly situated persons, allege the following against Ben E. Keith Company ("BEK" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

**I. DISCOVERY CONTROL PLAN**

Plaintiffs intends that discovery be conducted under Discovery Level 3 in accordance with Texas Rule of Civil Procedure 190.4 and requests that the Court enter a discovery control plan order tailored to the circumstances of this suit. This case is not subject to the restrictions of expedited discovery under Texas Rule of Civil Procedure 169 because the potential relief sought by the Plaintiffs and the putative class members in this action includes a claim for non-monetary injunctive and declaratory relief and claims for monetary relief including costs and attorneys' fees in excess of \$1,000,000.

## II. INTRODUCTION

1. Plaintiffs bring this class action against BEK for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former job applicants and employees' (collectively referred to herein as "Class Members") personally identifying information from hackers. According to the company, this information may have included names and Social Security numbers (the "Private Information") belonging to at least 39,789 Class Members.<sup>1</sup>

2. On or around March 14, 2023, BEK discovered a data security incident through which an unauthorized threat actor gained access to BEK's network and accessed files on its computer systems between March 3, 2023, and March 5, 2023 (the "Data Breach"). Through the Data Breach, the cybercriminals were able to access current and former job applicants' and employees' names and Social Security numbers.

3. As a result of the Data Breach, Plaintiffs and Class Members have experienced and/or are at a substantial and imminent risk of experiencing identity theft and various other forms of personal, social, and financial harm. This risk will remain for their respective lifetimes.

4. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, Social Security numbers that BEK collected from its current and former job applicants and employees and maintained in its systems. Compounding the damage done by the Data Breach, BEK failed to notify affected Class Members until nearly *seven months* after it discovered the Data Breach.

5. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain

---

<sup>1</sup> See <https://apps.web.maine.gov/online/aevviewer/ME/40/38510d88-ae1e-4d32-846c-6d1afb37b804.shtml> (last visited on November 14, 2023).

government benefits and/or medical services, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

6. There has been no assurance offered by BEK that all personal data or copies of data have been recovered or destroyed, or that it has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

7. Therefore, Plaintiffs and Class Members are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

8. Plaintiffs bring this class action lawsuit to address BEK's inadequate safeguarding of their and Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

9. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to BEK, and thus BEK was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

10. Plaintiffs' and Class Members' identities are now at risk because of BEK's negligent conduct because the Private Information that BEK collected and maintained is now in the hands of data thieves and other unauthorized third parties.

11. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

12. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, invasion of privacy, breach of implied contract, and unjust enrichment.

### **III. PARTIES**

13. Plaintiffs Jeremy P. Baca is an individual citizen of the State of Texas.

14. Plaintiff Dylan Lamoreaux is an individual citizen of the State of Texas.

15. Plaintiff Peter Salinas is an individual citizen of the State of Texas.

16. Plaintiff Curtis Lane is an individual citizen of the State of Texas.

17. Defendant is incorporated in Texas with its principal place of business located at 601 East 7<sup>th</sup> Street in Fort Worth, Texas, in Tarrant County.

### **IV. JURISDICTION AND VENUE**

18. 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.

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

20. This action is brought by Plaintiffs as a class action individually and on behalf of all others similarly situated under Rule 42 of the Texas Rules of Civil Procedure. Plaintiffs and the

putative class members seek nonmonetary injunctive, declaratory, and incident and subordinate relief and monetary relief including costs and attorneys' fees in excess of \$1,000,000.

## **V. FACTUAL ALLEGATIONS**

### ***A. BEK's Business and Collection of Plaintiffs' and Class Members' Private Information***

21. Founded in 1931, BEK is a food and beverage distribution company based in Fort Worth, Texas. Upon information and belief, BEK provides services in 15 states, employing more than 6,000 people and generating approximately \$5 billion in annual revenue.

22. As a condition of employment or submitting an application for employment with BEK, Defendant requires that individuals entrust it with highly sensitive personal information, including but not limited to, social security numbers. In the ordinary course of employment or applying for employment with BEK, Plaintiffs and Class Members were required to provide this and other sensitive personal information to Defendant.

23. Because of the highly sensitive and personal nature of the information BEK acquires and stores with respect to its employees and job applicants, BEK, upon information and belief, promises to, among other things, keep employees' and job applicants' Private Information private; comply with industry standards related to data security and the maintenance of employee and applicant Private Information; inform its employees and applicants of its legal duties relating to data security and comply with all federal and state laws protecting employee/applicant Private Information; only use and release employees' and applicants' Private Information for reasons that relate to the services it provides; not store former employees' or applicants' Private Information for longer than is necessary to carry out its business operations; and provide adequate notice to its current and former employees and applicants if their Private Information is disclosed without authorization.

24. By obtaining, collecting, using, and deriving a benefit from its employees' and applicants' Private Information, BEK assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

25. Plaintiffs and Class Members relied on BEK to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

***B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members***

26. In the Notice letter that went out to all impacted current and former BEK employees and applicants on or around October 26, 2023, Defendant reported that it learned of unauthorized access to its computer systems approximately *seven months* earlier on or around March 14, 2023. Based upon the company's investigation, it discovered that the Data Breach was the result of an attack on its systems that allowed an "unauthorized actor" to gain access to its systems and ultimately access copies of Plaintiffs' and Class Members' Private Information. It is clear that the data thieves carried out this attack in order to either use the Private Information themselves for nefarious purposes, or to sell it on the dark web.

27. Thus, through the Data Breach, the unauthorized cybercriminal(s) accessed and exfiltrated a cache of highly sensitive Private Information, including BEK's current and former employees' and applicants' names and Social Security numbers.

28. BEK had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

29. Plaintiffs and Class Members provided their Private Information to BEK with the reasonable expectation and mutual understanding that BEK would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

30. BEK's data security obligations were particularly important given the substantial increase in cyberattacks carried out against employers in recent years.

31. BEK knew or should have known that its electronic records would be targeted by cybercriminals, yet it failed to take the necessary precautions to protect Plaintiffs' and Class Members' Private Information from being compromised.

32. In response to its admitted failure to safeguard Plaintiffs' and Class Members' Private Information, BEK's response is particularly paltry. In its Notice, Defendant offered Plaintiffs just 2 years of credit monitoring.

### ***C. BEK Failed to Comply with FTC Guidelines***

33. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

34. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that 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 into 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.

35. The FTC further recommends that companies not maintain personally identifiable information ("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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. As evidenced by the Data Breach, BEK failed to properly implement basic data security practices. BEK's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information evidences its negligent failure to comply with the standards set forth by Section 5 of the FTCA.

38. BEK was at all times fully aware of its obligation to protect the Private Information of its current and former employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

#### ***D. BEK Failed to Comply with Industry Standards***

39. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

40. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.<sup>2</sup>

41. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

- a. Control who logs on to your network and uses your computers and other devices.
- b. Use security software to protect data.
- c. Encrypt sensitive data, at rest and in transit.
- d. Conduct regular backups of data.
- e. Update security software regularly, automating those updates if possible.
- f. Have formal policies for safely disposing of electronic files and old devices.
- g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

---

<sup>2</sup> *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, <https://www.cisecurity.org/controls/cis-controls-list> (last visited on Nov. 15, 2024).

42. Further still, the United States Cybersecurity and Infrastructure Security Agency (“CISA”) makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that “remote access to the organization’s network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization’s IT personnel have disabled all ports and protocols that are not essential for business purposes,” and other steps; (b) taking steps to quickly detect a potential intrusion, including “[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization’s entire network is protected by antivirus/antimalware software and that signatures in these tools are updated,” and (c) “[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs,” and other steps.<sup>3</sup>

43. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet one or more of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to

---

<sup>3</sup> *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/shields-guidance-organizations> (last visited Nov. 15, 2024).

comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

***E. BEK Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information***

44. In addition to its obligations under federal and state laws, BEK owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. BEK owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of its current and former employees.

45. BEK breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. BEK's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect current and former employees' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- e. Failing to adhere to industry standards for cybersecurity as discussed above; and
- f. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

46. BEK negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information and exfiltrate such Private Information.

47. Had BEK remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

48. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

***F. BEK Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft***

49. The FTC hosted a workshop to discuss "informational injuries," which are injuries that current and former employees like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.<sup>4</sup> Exposure of highly sensitive personal information that individuals to keep private may cause harm to them, such as the ability to obtain or keep employment. Individuals' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

50. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to

---

<sup>4</sup> *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), available at [https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational\\_injury\\_workshop\\_staff\\_report\\_-\\_oct\\_2018\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf) (last visited on November 14, 2023).

monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

51. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

52. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

53. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

54. One such example of this is the development of "Fullz" packages.

55. Cybercriminals can cross-reference two sources of the Private Information

compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

56. The development of “Fullz” packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and the proposed Class’s phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members’ stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

57. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim’s identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.<sup>5</sup> However, these steps do not guarantee protection from identity theft but can only mitigate identity theft’s long-lasting negative impacts.

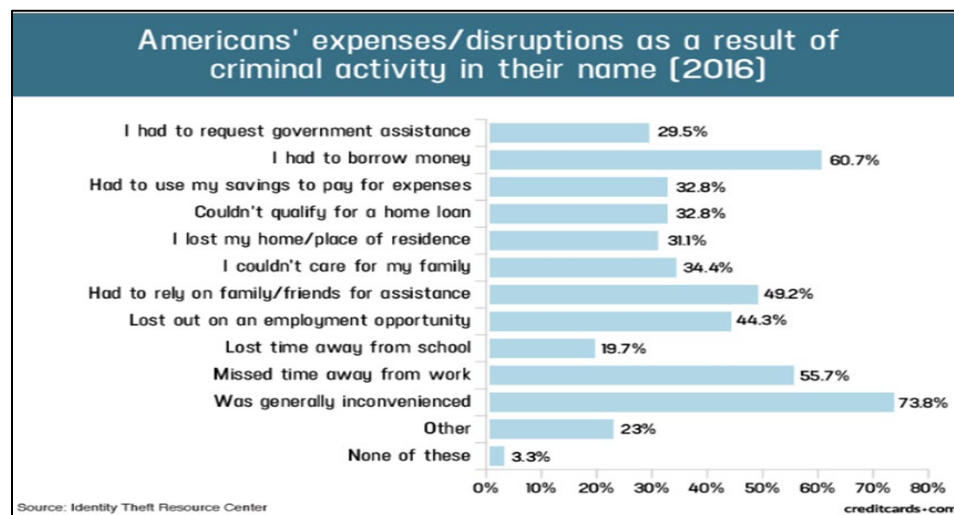
58. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud,

---

<sup>5</sup> See *IdentityTheft.gov*, Federal Trade Commission, available at <https://www.identitytheft.gov/Steps> (last visited on November 14, 2023).

to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to 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 in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

59. A study by the Identity Theft Resource Center<sup>6</sup> shows the multitude of harms caused by fraudulent use of PII:



60. Indeed, a robust cyber black market exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

61. The value of such highly sensitive information is axiomatic. The value of “big data” in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that PII has considerable market value.

<sup>6</sup> Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/> (last visited April 27, 2023).

62. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:<sup>7</sup>

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

63. PII is a valuable commodity to identity thieves because once the information has been compromised, criminals often trade the information on the “cyber black market” for years.

64. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future and have no choice but to vigilantly monitor their accounts and purchase credit monitoring and identity theft protection for many years to come.

### ***G. Plaintiffs’ and Class Members’ Experience and Resulting Damages***

#### *Plaintiffs Baca’s Experience*

65. Plaintiffs Baca is a former job applicant of Defendant. As a condition of seeking employment with Defendant, Plaintiffs Baca was required to give his Private Information to Defendant.

66. Plaintiffs Baca is very careful about sharing his Private Information. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiffs Baca stores any documents containing his sensitive PII in a safe and secure location or destroys the documents.

---

<sup>7</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at <https://www.gao.gov/assets/270/262904.html> (last visited May 25, 2023).

67. Plaintiffs Baca only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

68. Plaintiff Baca received the Notice of Data Breach on or around October 26, 2023, stating, in relevant part, that his name and Social Security number was disclosed in the Data Breach.

*Plaintiff Lamoreaux's Experience*

69. Plaintiff Lamoreaux entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information. Plaintiff Lamoreaux would not have allowed Defendant's financial services to collect and maintain his Private Information had he known that Defendant would not take reasonable steps to safeguard his Private Information.

70. Plaintiff Lamoreaux 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 calls, 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.

71. Plaintiff Lamoreaux stores all documents containing his Private Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

72. Plaintiff Lamoreaux has suffered actual injury in the form of damages to, and diminution in, the value of his Private Information – a form of intangible property that Plaintiff

entrusted to Defendant. This Private Information was compromised in, and has been diminished as a result of, the Data Breach.

73. Plaintiff Lamoreaux has also suffered actual injury in the forms of uncompensated 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.

74. Plaintiff Lamoreaux has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Private Information resulting from the compromise of his Private Information, especially his SSN, in combination with his name, which is now in the hands of cyber criminals and other unauthorized third parties.

75. Knowing that thieves stole his Private Information, including his SSN, and knowing that his Private Information will likely be sold on the dark web, has caused Plaintiff great anxiety.

76. Additionally, Plaintiff Lamoreaux does not recall having been involved in any other data breaches in which his sensitive and confidential Private Information, such as his SSN, was compromised.

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

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

#### *Plaintiff Salinas's Experience*

79. Plaintiff Salinas is a former employee at Ben Keith who worked there from approximately 2015 to 2018.

80. As a condition of his employment at Ben Keith, he was required to supply Defendant with his PII, including but not limited to his name and Social Security number.

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

82. At the time of the Data Breach—March 3, 2023 through March 5, 2023—Defendant retained Plaintiff’s PII in its system.

83. Plaintiff Salinas received the Notice Letter, by U.S. mail, directly from Defendant, dated October 26, 2023. According to the Notice Letter, Plaintiff’s PII was improperly accessed and obtained by unauthorized third parties, including his full name and Social Security number.

84. As a result of the Data Breach, and at the direction of Defendant’s Notice Letter,<sup>8</sup> Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring their own computer networks, and signing up for the credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent significant on mitigation activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

---

<sup>8</sup> “We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*. There you will find more information on the complimentary credit monitoring services that we are offering to you.” See Notice Letter.

85. Subsequent to the Data Breach, Plaintiff Salinas has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

86. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

87. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

88. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

#### *Plaintiff Lane's Experience*

90. Plaintiff Curtis Lane is an adult individual and, at all relevant times herein, a resident and citizen of Texas, residing in Paris, Texas. Plaintiff Lane is a victim of the Data Breach.

91. Plaintiff Lane is a former employee of Defendant's, and his information was stored with Defendant as a result of their dealings with Defendant.

92. As required in order to obtain services from Defendant, Plaintiff Lane provided Defendant with highly sensitive personal and financial information, who then possessed and controlled it.

93. As a result, Plaintiff Lane's information was among the data accessed by an unauthorized third-party in the Data Breach.

94. At all times herein relevant, Plaintiff Lane is and was a member of the Class.

95. Plaintiff Lane received a letter from Defendant, dated October 26, 2023, stating that their PII and/or financial information was involved in the Data Breach (the "Notice").

96. Plaintiff Lane was unaware of the Data Breach—or even that Defendant had possession of their data until receiving that letter.

97. As a result, Plaintiff Lane was injured in the form of uncompensated lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

98. Plaintiff Lane was also injured by the material risk to future harm he suffers based on Defendant's breach; this risk is imminent and substantial because Plaintiff Lane's data has been exposed in the breach, the data involved, including Social Security numbers, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

99. Plaintiff Lane suffered actual injury in the form of damages to and diminution in the value of their PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

100. Plaintiff Lane’s finances have already been impacted by this breach. In mid-March 2023, Plaintiff Lane experienced an unauthorized \$25 on his credit card and a bill for \$1,000 worth of medical services Plaintiff Lane did not receive. The information involved in these fraudulent charges were implicated in the Data Breach and occurred after the Data Breach.

101. Plaintiff Lane, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PII and/or financial information.

102. Plaintiff Lane has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and financial information, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

103. Plaintiff Lane has a continuing interest in ensuring that their PII and financial information, which, upon information and belief, remains backed up in Defendant’s possession, is protected and safeguarded from future breaches.

*Plaintiffs’ and Class Members’ Experience*

104. In sum, Plaintiffs and Class Members are at an imminent, immediate, and continuing increased risk of experiencing devastating instances of identity theft, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, unauthorized charges made on their financial accounts, and other forms of identity theft.

105. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to continue to carry out such targeted schemes against Plaintiffs and Class Members.

106. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which has been and will continue to be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

107. Further, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach. Specifically, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

108. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

109. Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200

billion.<sup>9</sup> In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$50 a year.<sup>10</sup>

110. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

111. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

112. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of BEK, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

---

<sup>9</sup> See <https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion>. (last visited on November 14, 2023).

<sup>10</sup> *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited on November 14, 2023).

113. As a direct and proximate result of BEK's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

## **VI. CLASS ACTION ALLEGATIONS**

114. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Texas Rule of Civil Procedure 42.

115. Specifically, Plaintiffs propose the following Class (referred to herein as the "Class"), subject to amendment as appropriate:

**All individuals in the United States whose Private Information was accessed and/or acquired in the Data Breach, including all who were sent a notice of the Data Breach.**

116. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

117. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class as well as to add subclasses before the Court determines whether certification is appropriate.

118. The proposed Class meets the criteria for certification under Texas Rule of Civil Procedure 42, as further set forth below.

119. 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, based on information and belief, the Class consists of at least 39,789 current and former employees and job applicants of BEK whose data was compromised in the Data Breach. The identities of

Class Members are ascertainable through BEK's records, Class Members' records, publication notice, self-identification, and other means.

120. 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:

- a. Whether BEK engaged in the conduct alleged herein;
- b. When BEK learned of the Data Breach;
- c. Whether BEK's response to the Data Breach was adequate;
- d. Whether BEK unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
- e. Whether BEK failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- f. Whether BEK's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- g. Whether BEK's data security systems prior to and during the Data Breach were consistent with industry standards;
- h. Whether BEK owed a duty to Class Members to safeguard their Private Information;
- i. Whether BEK breached its duty to Class Members to safeguard their Private Information;
- j. Whether hackers exfiltrated Class Members' Private Information via the Data Breach;

- k. Whether BEK had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
- l. Whether BEK breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- m. Whether BEK knew or should have known that its data security systems and monitoring processes were deficient;
- n. What damages Plaintiffs and Class Members suffered as a result of BEK's misconduct;
- o. Whether BEK's conduct was negligent;
- p. Whether BEK was unjustly enriched;
- q. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

121. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

122. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

123. Predominance. BEK has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from BEK'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.

124. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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 BEK. In contrast, conducting 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.

125. Finally, all members of the proposed Class are readily ascertainable. BEK has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by BEK.

## **CLAIMS FOR RELIEF**

### **COUNT I NEGLIGENCE**

#### **(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

126. Plaintiffs restate and reallege allegations stated above as if fully set forth herein.

127. BEK knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

128. BEK knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. BEK was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

129. BEK owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. BEK's duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect current and former employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA and applicable industry standards;
- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. To precisely disclose the type(s) of information compromised.

130. BEK's duty to employ reasonable data security measures arose, in part, 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.

131. BEK's duty also arose because Defendant was bound by industry standards to protect its current and former employees' and job applicants' confidential Private Information.

132. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and BEK owed them a duty of care not to subject them to an unreasonable risk of harm.

133. BEK, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within its possession.

134. BEK, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

135. BEK breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to comply with the FTCA and applicable industry standards;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- f. 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.

136. BEK had a special relationship with its current and former employees and job applicants, including Plaintiffs and Class Members.

137. Plaintiffs' and Class Members' willingness to entrust BEK with their Private Information was predicated on the understanding that BEK would take adequate security precautions to protect it. Moreover, only BEK had the ability to protect its systems (and the Private Information stored thereon) from attack.

138. BEK's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein and admitted by Defendant in its Notice to Plaintiffs and Class Members.

139. BEK's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

140. As a result of BEK's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of criminal third parties, has been and will continue to be used for fraudulent purposes.

141. BEK also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information.

142. As a direct and proximate result of BEK's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

143. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

144. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

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

**COUNT II**  
**INVASION OF PRIVACY**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

146. Plaintiffs restate and reallege allegations stated above as if fully set forth herein.

147. Plaintiffs and Class Members maintain a privacy interest in their Private Information, which is highly sensitive, confidential information that is also protected from disclosure by applicable laws and industry standards, as set forth above.

148. Plaintiffs' and Class Members' Private Information was contained, stored, and managed electronically in Defendant's records, computers, and databases and was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiffs' and Class Members' identities were only shared with Defendant for the limited purpose of obtaining employment.

149. Additionally, Plaintiffs' and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

150. Defendant's disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties by allowing such parties to gain access to its network resulted from Defendant's failure to adequately secure and safeguard Plaintiffs' and Class Members' Private Information. Such failure was the direct and proximate cause of unauthorized intrusions into Plaintiffs' and Class Members' places of solitude and seclusion that are highly offensive to a reasonable person.

151. Such exploitation of Plaintiffs' and Class Members' Private Information was done for Defendant's business purposes.

152. BEK's unauthorized disclosure of Plaintiffs' and Class Members' Private Information to criminal third parties permitted the electronic intrusion into private quarters where Plaintiffs' and Class Members' Private Information was stored.

153. Plaintiffs and Class Members have been damaged by BEK's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

**COUNT III**  
**BREACH OF IMPLIED CONTRACT**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

154. Plaintiffs restate and reallege allegations stated above as if fully set forth herein.

155. BEK provided employment to Plaintiffs and Class Members.

156. Defendant, as employer, held the Private Information on behalf of Plaintiffs and Class Members. Holding Plaintiffs' and Class Members' Private Information was part of Defendant's regular business practices, as agreed by the parties. When Plaintiffs and Class Members joined Defendant's employment, they agreed to have their Private Information stored in Defendant's network.

157. Plaintiffs and Class Members entered implied contracts with Defendant in which Defendant agreed to safeguard and protect such Information and to timely detect any breaches of their Private Information. Plaintiffs and Class Members were required to share Private Information to obtain employment. In entering such implied contracts, Plaintiffs 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.

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

159. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that

is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

160. Defendant breached these implied promises it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to notify Plaintiffs and Class Members thereof within a reasonable time.

161. Plaintiffs and Class Members would not have entrusted their Private Information to BEK in the absence of such an implied contract.

162. Had BEK disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices in place to secure such sensitive data, Plaintiffs and Class Members would not have provided their Private Information to BEK.

163. BEK recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

164. BEK violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

165. Plaintiffs and Class Members have been damaged by BEK's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

166. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (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 free lifetime credit monitoring to all Class Members.

**COUNT IV**  
**UNJUST ENRICHMENT**  
**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

167. Plaintiffs restate and reallege allegations stated above as if fully set forth herein.

168. This Count is pleaded in the alternative to Count III above.

169. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to have Defendant protect their Private Information with adequate data security, especially in light of their employer-employee relationship.

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

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

172. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate security practices previously alleged.

173. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to secure their Private Information, they would have made alternative employment choices that excluded Defendant.

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

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

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

177. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from BEK and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by BEK from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

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

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

- a. An order certifying this action as a Class action under Tex. R. Civ. P. 42, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;
- b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing BEK to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
- e. An order requiring BEK to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

## DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 25, 2024

Respectfully submitted,

*/s/ Joe Kendall*

---

JOE KENDALL

Texas Bar No. 11260700

**KENDALL LAW GROUP, PLLC**

3811 Turtle Creek Blvd., Suite 825

Dallas, Texas 75219

214-744-3000 / 214-744-3015 (Facsimile)

jkendall@kendalllawgroup.com

David DiSabato (admitted *pro hac vice*)

Tyler Bean (*pro hac vice* to be filed)

**SIRI & GLIMSTAD LLP**

745 Fifth Avenue, Suite 500

New York, New York 10151

Tel: (212) 532-1091

E: ddisabato@sirillp.com

E: tbean@sirillp.com

Gary Klinger (*pro hac vice* to be filed)

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN, PLLC**

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Telephone: (866) 252-0878

gklinger@milberg.com

Kevin Laukaitis (*pro hac vice* to be filed)

**LAUKAITIS LAW LLC**

954 Avenida Ponce De Leon

Suite 205, #10518

San Juan, PR 00907

T: (215) 789-4462

klaukaitis@laukaitislaw.com

Philip J. Krzeski (*pro hac vice* to be filed)

**CHESTNUT CAMBRONNE PA**

100 Washington Ave., Ste. 1700

Minneapolis, MN 55401-2138  
Tel: (612) 767-3613  
E: pkrzeski@chestnutcambronne.com

*Attorneys for Plaintiffs and the Class*

**CERTIFICATE OF SERVICE**

I hereby certify that a copy of the foregoing document was served on all counsel of record on November 25, 2024 via e-file Texas, in accordance with the Texas Rules of Civil Procedure.

/s/ Joe Kendall  
JOE KENDALL

### Automated Certificate of eService

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

Joe Kendall

Bar No. 11260700

administrator@kendalllawgroup.com

Envelope ID: 94690393

Filing Code Description: Amended Filing

Filing Description: Plaintiffs' First Amended Class Action Petition

Status as of 11/25/2024 4:21 PM CST

Associated Case Party: JEREMYPBACA

| Name            | BarNumber | Email                        | TimestampSubmitted    | Status |
|-----------------|-----------|------------------------------|-----------------------|--------|
| Joe Kendall     |           | jkendall@kendalllawgroup.com | 11/25/2024 3:53:28 PM | SENT   |
| David JDisabato |           | ddisabato@sirillp.com        | 11/25/2024 3:53:28 PM | SENT   |

Associated Case Party: THEBEN E KEITH COMPANY

| Name                 | BarNumber | Email                   | TimestampSubmitted    | Status |
|----------------------|-----------|-------------------------|-----------------------|--------|
| Christopher Norcross |           | cnorcross@grsm.com      | 11/25/2024 3:53:28 PM | SENT   |
| VLS DFW Support      |           | VLS_DFWSupport@grsm.com | 11/25/2024 3:53:28 PM | SENT   |
| Elleni Tesfaye       |           | etesfaye@grsm.com       | 11/25/2024 3:53:28 PM | SENT   |
| Sarah Anderson       |           | sjanderson@grsm.com     | 11/25/2024 3:53:28 PM | SENT   |
| Kortney West         |           | kwest@grsm.com          | 11/25/2024 3:53:28 PM | SENT   |

Case Contacts

| Name             | BarNumber | Email                          | TimestampSubmitted    | Status |
|------------------|-----------|--------------------------------|-----------------------|--------|
| Tyler Bean       |           | tbean@sirillp.com              | 11/25/2024 3:53:28 PM | SENT   |
| Alcira Pena      |           | apena@sirillp.com              | 11/25/2024 3:53:28 PM | SENT   |
| David DiSabato   |           | ddisabato@sirillp.com          | 11/25/2024 3:53:28 PM | SENT   |
| Helena Gurtu     |           | hgurtu@kendalllawgroup.com     | 11/25/2024 3:53:28 PM | SENT   |
| Gary Klinger     |           | gklinger@milberg.com           | 11/25/2024 3:53:28 PM | SENT   |
| Kevin Laukaitis  |           | klaukaitis@kaukaitislaw.com    | 11/25/2024 3:53:28 PM | SENT   |
| Philip J.Krzeski |           | pkrzeski@chestnutcambronne.com | 11/25/2024 3:53:28 PM | SENT   |
| Sandra Passanisi |           | spassanisi@milberg.com         | 11/25/2024 3:53:28 PM | SENT   |