

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

ALISHA BOYKIN, KRISTEN HANSEN,
TRACY MANGANO, AMY DITTBENNER,
LARA SULEIMAN and DUSICA PEREZ,

Plaintiffs

v.

PANERA BREAD COMPANY,

Defendant.

CIVIL ACTION 1:18-cv-02461

Judge -

JURY TRIAL DEMANDED

CLASS ACTION LAWSUIT

NOW COME the Plaintiffs, ALISHA BOYKIN, KRISTEN HANSEN, TRACY MANGANO, AMY DITTBENNER, LARA SULEIMAN and DUSICA PEREZ (at times “Plaintiffs”), by and through their attorney, James C. Vlahakis of the Sulaiman Law Group, Ltd., and bring this civil action against PANERA BREAD COMPANY (“Panera”) pursuant to Federal Rule of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4):

I. Introduction

1. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter “Class Members”), bring this class action to secure redress of Panera’s negligent and reckless violation of its customers’ privacy rights.

2. Plaintiffs and Class Members are former Panera customers who created and utilized (a) Panera’s My Rewards card and/or (b) an internet and smart phone app called MyPanera to order Panera food products for pickup orders.

3. Plaintiffs and Class Members are persons who purchased food and/or beverages at one of Panera’s approximately 2,000 nationwide restaurants during as yet undetermined time period where their names, credit and/or debit card account numbers, card expiration dates, card verification codes, emails, telephone numbers and

other demographic information (hereafter “Personal Identifying Information”) was negligently or recklessly exposed to hackers and/or unknown nefarious third parties.

4. As alleged below, Plaintiffs’ and Class Members’ Personal Identifying Information was vulnerable to hackers and and/or unknown nefarious third parties by Panera’s negligent and/or reckless conduct in how Panera managed its MyPanera and Rewards programs.

5. As alleged below, Plaintiffs and Class Members suffered real injuries as a result of Panera negligently or recklessly exposing their Personal Identifying Information Panera’s website to hackers and other as yet unknown nefarious third-parties.

6. On information and belief, personal identifying information may also have been stolen from Panera’s point-of-sale network as result of how Panera hosted and secured Personal Identifying Information in the MyPanera and Rewards programs.

7. In addition to the Plaintiffs, thousands of Panera’s customers have had their Personal Identifying Information leaked, stolen and/or compromised.

8. Accordingly, Plaintiffs, and thousands of Panera’s customers have had their privacy rights violated, have been exposed to the increased risk of fraud and identify theft, and have otherwise suffered damages.

II. Parties, Jurisdiction and Venue

9. Plaintiff ALISHA BOYKIN is a resident of the state of Tennessee and until recently was a resident of state of Indiana.

10. Plaintiff KRISTEN HANSEN is a resident of the state of Minnesota.

11. Plaintiff TRACY MANGANO is a resident of the state of Minnesota.

12. Plaintiff AMY DITTBENNER is a resident of the state of Illinois.

13. Plaintiff LARA SULEIMAN is a resident of the state of Illinois

14. Plaintiff DUSICA PEREZ is a resident of the state of Illinois.

15. Plaintiffs have utilized MyPanera accounts to purchase food on-line for pickup at a local Panera restaurant in their respective states and/or they have utilized their Panera Rewards accounts to obtain “points” for purchases.

16. Each of the Plaintiffs provided Panera with some form of their Personal Identifying Information in conjunction with their creation and use of their respective Meet MyPanera or/or Panera Rewards accounts.

17. Each of the Plaintiffs provided Panera with their credit card information either in initially setting up their MyPanera account, in updating their MyPanera account on when the paid for food at Panera restaurant after making an on-line or in-store order through their respective MyPanera or Panera Rewards accounts.

18. Defendant Panera Bread Company (“Panera”) is a Delaware corporation with its principal place of business in St. Louis, Missouri.

19. This Court has subject matter jurisdiction over the state law claims asserted here pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendant and, upon the original filing of this complaint, members of the putative Plaintiff class resided in states around the country; there are more than 100 putative class members; and the amount in controversy exceeds \$5 million.

20. The Court also has personal jurisdiction over the Parties because Panera has conducted and continues to conduct substantial business in Illinois, it is authorized to conduct business throughout the United States, including Illinois; and it advertises in a variety of media throughout the United States, including Illinois.

21. Via its business operations throughout the United States, Panera intentionally avails itself of the markets within this state to render the exercise jurisdiction by this Court just and proper.

22. Venue is appropriate in this district because, among other things: (a) one or more of the Plaintiffs is a resident of this district; (b) Panera has restaurants in in this district; (c) one or more of the Plaintiffs ate at or purchased food and beverages from a Panera restaurant in this district; (d) some of the acts and omissions that give rise to this civil action took place in this district; and (e) one or more of the Plaintiffs suffered harm in this district as a result of Panera's negligence or recklessness.

23. Venue is further appropriate pursuant to 28 U.S.C. § 1391 because Panera conducts a large amount of their business in this district, Defendant has substantial relationships in this District and one or more of the Plaintiffs reside in this district.

24. Venue is also proper in this Court because a substantial part of the events and omissions giving rise to the harm of the Class Members occurred in this district.

III. Background Information – Why Our Personal Identifying Information and Personal Identifying Information Should Be Protected By Companies We Do Business With

25. Personal Identifying Information, and in particular, credit and debit card data is highly coveted and a frequent target of hackers.

26. Hackers also value emails and telephone numbers as they allow hackers to reset passwords.

27. Despite well-publicized litigation and frequent public announcements of data breaches by retailers, Panera opted to maintain an insufficient and inadequate system to protect the Personal Identifying Information of Plaintiffs and Class Members.

28. Criminal underground alike recognize the value of Personal Identifying Information and payment information. Otherwise, they would not aggressively seek or pay for it.

29. Some companies, like Uber, for instance, have even secretly paid off hackers to cover-up the fact that hackers had accessed personal information related to

57 worldwide Uber drivers and riders. <https://thehackernews.com/2017/12/uber-hacker.html>

30. 40 Millions Target customers were impacted by a credit card data breach. <http://money.cnn.com/2013/12/18/news/companies/target-credit-card/>

31. Credit or debit card information is highly valuable to hackers. Credit and debit card information that is stolen from the point of sale are known as “dumps.” See KREBS ON SECURITY April 16, 2016, <https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/>

32. Credit and debit card dumps can be sold in the cybercrime underground for a retail value of about “\$20 apiece.” *Id.*

33. This information can also be used to clone a debit or credit card. *Id.*

34. According to Javelin Strategy and Research, “one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year.” See, “Someone Became an Identity Theft Victim Every 2 Seconds Last Year,” Fox Business, Feb. 5, 2014, <http://www.foxbusiness.com/personalfinance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-lastyear.html>

35. It takes time for consumers to fix and repair their credit after it has been compromised by nefarious third parties.

36. The Department of Justice’s Bureau of Justice Statistics (“BJS”) found that “among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.” See “Victims of Identity Theft,” U.S. Department of Justice, Dec 2013, <https://www.bjs.gov/content/pub/pdf/vit12.pdf>

37. The BJS reported, “resolving the problems caused by identity theft [could] take more than a year for some victims.” *Id.* at 11.

38. Just as there is often a time lag between a data breach or leak of Personal Identifying Information occurs and when it is discovered, there is a time lag between when Personal Identifying Information is stolen and when it is used.

39. In 2007, the U.S. Government Accountability Office (“GAO”) conducted a Report to Congressional Requesters regarding data breaches and reported the following:

[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.

<http://www.gao.gov/new.items/d07737.pdf> (at page 33).

IV. Factual Allegations

40. Panera was warned that it had placed sensitive personal information of customers at risk but Panera ignored the warning.

41. On April 2, 2018, KREBS ON SECURITY reported that Panera’s website had “leaked millions of customer records - including names, email and physical addresses, birthdays and the last four digits of the customer’s credit card number - for at least eight months before it was yanked offline earlier today.”

42. The KREBS ON SECURITY Blog Post can be found here <https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/>

43. According to KREBS ON SECURITY :

The data available in plain text from Panera’s site appeared to include records for any customer who has signed up for an account to order food online via panerabread.com. The St. Louis-based company, which has more than 2,100 retail locations in the United States and Canada, allows customers to order food online for pickup in stores or for delivery.

* * *

KrebsOnSecurity learned about the breach earlier today after being contacted by security researcher **Dylan Houlihan**, who said he initially notified Panera about customer data leaking from its Web site back on August 2, 2017.

A long message thread that Houlihan shared between himself and Panera indicates that **Mike Gustavison**, Panera's director of information security, initially dismissed Houlihan's report as a likely scam. A week later, however, those messages suggest that the company had validated Houlihan's findings and was working on a fix.

"Thank you for the information we are working on a resolution," Gustavison wrote.

Mike,

Can you confirm that you have been able to decrypt and verify the report?

Best,
Dylan

From: Mike Gustavison <Mike.Gustavison@panerabread.com>
Date: Wed, Aug 9, 2017 at 11:02 AM
To: Dylan Houlihan <[dylan\[REDACTED\]](mailto:dylan[REDACTED])>

Yes sir...

Thank you for the information we are working on a resolution.

Mike

From: Dylan Houlihan [mailto:[dylan\[REDACTED\]](mailto:dylan[REDACTED])]
Sent: Monday, August 07, 2017 9:47 PM

Fast forward to early this afternoon — exactly eight months to the day after Houlihan first reported the problem — and data shared by Houlihan indicated the site was still leaking customer records in plain text. Worse still, the records could be indexed and crawled by automated tools with very little effort.

For example, some of the customer records include unique identifiers that increment by one for each new record, making it potentially simple for someone to scrape all available customer accounts. The format of the database also lets anyone search for customers via a variety of data points, including by phone number.

"Panera Bread uses sequential integers for account IDs, which means that if your goal is to gather as much information as you can instead about someone, you can simply increment through the accounts and collect as much as you'd like, up to and including the entire database," Houlihan said.

Asked whether he saw any indication that Panera ever addressed the issue he reported in August 2017 until today, Houlihan said no.

“No, the flaw never disappeared,” he said. “I checked on it every month or so because I was pissed.”

Shortly after KrebsOnSecurity spoke briefly with Panera’s chief information officer **John Meister** by phone today, the company briefly took the Web site offline. As of this publication, the site is back online but the data referenced above no longer appears to be reachable.

Another data point exposed in these records included the customer’s Panera loyalty card number, which could potentially be abused by scammers to spend prepaid accounts or to otherwise siphon value from [Panera customer loyalty accounts](#).

It is not clear yet exactly how many Panera customer records may have been exposed by the company’s leaky Web site, but incremental customer numbers indexed by the site suggest that number may be higher than seven million. It’s also unclear whether any Panera customer account passwords may have been impacted.

In a written statement, Panera said it had fixed the problem within less than two hours of being notified by KrebsOnSecurity. But Panera did not explain why it appears to have taken the company eight months to fix the issue after initially acknowledging it privately with Houlihan.

“Panera takes data security very seriously and this issue is resolved,” the statement reads. “Following reports today of a potential problem on our website, we suspended the functionality to repair the issue. Our investigation is continuing, but there is no evidence of payment card information nor a large number of records being accessed or retrieved.”

[HTTPS://KREBSONSECURITY.COM/2018/04/PANERABREAD-COM-LEAKS-MILLIONS-OF-CUSTOMER-RECORDS](https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records)

44. Notably, according to Mike Gustavison’s LinkedIn page, he worked at Equifax between January 2009 and June 2013, as its Sr. Director of Security Operations. See, <https://www.linkedin.com/in/mike-gustavison-b020426/>

45. Forbes.com reports that Equifax was subject to a data breach in 2013 when Mike Gustavison worked as Equifax’s Sr. Director of Security Operations:

Going further back four years, Equifax [reported](#) to the New Hampshire attorney general of a breach, admitting that between April 2013 and January 2014, an "IP address operator was able to obtain the credit reports using sufficient personal information to meet Equifax's identity verification process." There were other smaller data leaks reported by Equifax to the AG, though they only appeared to affect a handful of people.

<https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#66377e76677c>

46. According to KREBS ON SECURITY'S Blog Post, the following is an impage of what the leaked data looked like:



```
{ "accounts": [ { "username": "[REDACTED]", "name": "[REDACTED]", "cardNumber": "*****6515" }, { "username": "[REDACTED]@hotmail.com", "name": "[REDACTED]", "cardNumber": "*****5527" }, { "username": "[REDACTED]@msn.com", "name": "F B", "cardNumber": "*****7921" }, { "username": "[REDACTED]@yahoo.com", "name": "C", "cardNumber": "*****7108" }, { "username": "[REDACTED]", "cardNumber": "*****6129" }, { "username": "[REDACTED]@aol.com", "name": "[REDACTED]", "cardNumber": "*****6061" }, { "username": "[REDACTED]@yahoo.com", "name": "[REDACTED]", "cardNumber": "*****8950" }, { "username": "k", "name": "[REDACTED]", "cardNumber": "*****4412" }, { "username": "[REDACTED]", "name": "[REDACTED]", "cardNumber": "*****8386" }, { "username": "[REDACTED]@aol.com", "name": "[REDACTED]", "cardNumber": "*****5384" }, { "username": "[REDACTED]@optonline.net", "name": "[REDACTED]", "cardNumber": "*****5144" }, { "username": "[REDACTED]@hotmail.com", "name": "[REDACTED]", "cardNumber": "*****7488" }, { "username": "[REDACTED]", "name": "[REDACTED]", "cardNumber": "*****6702" }, { "username": "[REDACTED]", "name": "[REDACTED]", "cardNumber": "*****7085" }, { "username": "[REDACTED]@hotmail.com", "name": "[REDACTED]", "cardNumber": "*****4220" }, { "username": "[REDACTED]", "name": "[REDACTED]", "cardNumber": "*****9123" }, { "username": "art", "name": "[REDACTED]", "cardNumber": "*****8139" }, { "username": "[REDACTED]", "name": "[REDACTED]", "cardNumber": "*****0102" }, { "username": "[REDACTED]@msn.com", "name": "Sandra", "cardNumber": "*****6851" }, { "username": "k", "name": "[REDACTED]", "cardNumber": "*****2654" } ] }
```

47. Additionally, a Panera customer has posted that he warned Panera of a potential data breach in May of 2007.

48. According to “Jeff”, he received an unwanted solicitation email from a third-party marketer in an email account that he specifically earmarked for his Panera Rewards account.

49. “Jeff” noted that the marketing email was notable because it was related to a competitor of Panera.

50. When “Jeff” told Panera that he thought his account had been compromised “they blew me off.”

51. Panera has not fully disclosed the data leak on its website as of the time of the filing of this civil action.

52. Upon information and belief, Panera has taken no other efforts since discovering the security breach to inform customers that their Personal Identifying Information was leaked and/or compromised.

53. Panera failed to implement and maintain reasonable security procedures and practices appropriate to the protect the nature and scope of the information compromised in the data breach and/or leak.

54. As discussed in the above section and as discussed below, the ramification of Panera's failure to keep Plaintiffs' and Class Members' Personal Identifying Information secure is severe.

55. The data breach and/or leak was a direct and proximate result of Panera's failure to properly safeguard and protect Plaintiffs' and Class Members' Personal Identifying Information from unauthorized access, capture, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law.

56. Among other things, Panera failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Personal Identifying Information.

57. Panera failed to protect against reasonably foreseeable threats to the security or integrity of Plaintiffs' and Class Members' Personal Identifying Information.

58. Plaintiffs' and Class Members' Personal Identifying Information is private and sensitive in nature and was inadequately protected by Panera.

59. Panera did not obtain Plaintiffs' and Class Members' consent to disclose their Personal Identifying Information, except to certain persons not relevant to this action, as required by applicable law and industry standards.

60. As a direct and proximate result of Panera's wrongful action and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

61. Plaintiffs and Class Members will be required to spend time and resources to cancel every debit and/or credit card linked to their MyPanera app. Rewards account or otherwise used at any Panera location.

62. Plaintiffs and Class Members will be required to spend time and resources to monitor his or her credit reports to be on the lookout for fraud and/or identity theft.

63. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

64. Plaintiffs and the Class Members have and will incur monetary costs though hiring legal counsel to protect their good credit, reputations and rights.

65. Plaintiffs and Class Members now face years of increased risk loss of use of their credit and access to funds, including fraudulent and unreimbursed credit card charges.

66. Panera's wrongful actions and inaction directly and proximately caused the, display, disclosure, leakage, theft and dissemination into the public domain of Plaintiffs' and Class Members' Personal Identifying Information.

67. Panera's conduct has called Plaintiffs and Class Members to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. Theft of their personal and financial information;
- b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class Members' information on the Internet black market;
- c. The untimely and inadequate notification of the data breach;
- d. The improper disclosure of their Personal Identifying Information;
- e. Loss of privacy;
- f. Ascertainable losses 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; Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information, for which there is a well-established national and international market;
- g. Overpayments to Panera for products purchased during the subject data breach in that a portion of the price paid for such products by Plaintiffs and Class Members to Panera was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Personal Identifying Information, which Panera did not implement and, as a result, Plaintiffs and Class Members did not receive what they paid for and were overcharged by Panera; and
- h. Deprivation of rights they possess under state law.

V. Causes of Action

68. Plaintiffs incorporate the above paragraphs as if fully set forth below.

69. Plaintiffs bring this action on his own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of a Nationwide class and/or statewide classes in the states where they reside.

Count I - Violation of the Illinois Personal Information Protection Act

70. For the sake of judicial economy, Plaintiffs incorporate all of the above paragraphs into this Count as if fully set forth.

71. The Illinois Personal Information Protection Act (“IPIPA”) requires data collectors to inform Illinois citizens and state officials of data breaches. See, 815 ILCS 530/1, et. seq.

72. The IPIPA requires data collectors to inform Illinois citizens and state officials of data breaches.

73. Section 530/10 states as follows:

The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

74. Panera is a “data collector” as defined by the IPIPA because it handles, collects, disseminates and otherwise deals with nonpublic personal data.

75. The events described in this civil action constitute a "breach of the security of the system data" because Defendants’ misconduct led to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by Panera.

76. As set forth above, Panera allowed “personal information” as defined by the IPIPA to be disclosed, leaked, accessed, viewed or otherwise misappropriated by unknown third parties, because on information and belief, the information disclosed, leaked, accessed, viewed or otherwise misappropriated by nefarious third-parties includes the names of the Plaintiffs and Class Members and their account numbers, user names, emails and password prompts and last four digits of their credit or debit cards.

77. Panera violated the IPIPA by failing to disclose the data breach as required by Section 530/10.

78. Panera violated the IPIPA because as of the filing of this civil action, no disclosure notification was “made in the most expedient time possible and without unreasonable delay.”

79. Panera violated the IPIPA because the disclosure notification was not “consistent with any measures necessary to determine the scope of the breach.”

80. Panera violated the IPIPA because the disclosure notification was not “consistent with any measures necessary to . . . restore the reasonable integrity, security, and confidentiality of the data system.”

81. Panera hid the data leak from customers.

82. A violation of the IPIPA constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act (“ICFA”), 815 ILCS § 505/1, et. seq.

83. Further, Section 2 of ICFA prohibits, *inter alia*, deceptive and unfair conduct, including but not limited to, false representations, false statements and omissions.

84. Section 2 provides that:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice ... in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

85. Under the ICFA, an unfair act or practice is one that (a) offends public policy; (b) is immoral, unethical, oppressive or unscrupulous; or (c) causes substantial injury to consumers.

86. Panera's misconduct (a) offends public policy; (b) is immoral, unethical, oppressive or unscrupulous; and/or (c) has caused substantial injury to consumers.

87. Panera's misconduct has led to data breaches and the disclosure of personal information.

88. As discussed above, Plaintiffs have been harmed by Panera's conduct.

89. Plaintiffs would not have signed up for MyPanaera or Panera Rewards if they had known that their personal information was at risk as a result of Panera's lack security protocols.

90. Plaintiffs would have stopped using MyPanaera or Panera Rewards if they had known that their personal information had been breached as a result of Panera's lack security protocols.

WHEREFORE, Plaintiffs and Class Members residing in Illinois are entitled to declaratory relief, damages, attorney's fees, injunctive relief and equitable relief to remedy the above described misconduct.

Count II - Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA")

91. For the sake of judicial economy, Plaintiffs incorporate all of the above paragraphs into this Count as if fully set forth.

92. Panera's conduct violates ICFA.

WHEREFORE, because Panera violated ICFA, Plaintiffs and Class Members residing in Illinois are entitled to declaratory relief, damages, attorney's fees, injunctive relief and equitable relief to remedy the above described misconduct.

Count III –Tort of Intrusion Upon Seclusion

93. For the sake of judicial economy, Plaintiffs incorporate all of the above paragraphs into this Count as if fully set forth.

94. Under common law, a tort of Intrusion Upon Seclusion is committed where a person or entity intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.

95. Any such person or entity is subject to liability to the other for invasion of his or her privacy, if the intrusion would be highly offensive to a reasonable person.

96. Panera's misconduct has led to data breaches and the disclosure of personal information, including, possible pick up and drop off points for rides paid for through Uber's rideshare app.

97. Plaintiffs had a reasonable expectation that Panera would not compromise their Personal Identifying Information.

98. Panera's misconduct and resultant data disclosures was objectively unreasonable.

99. Accordingly, Panera intruded upon the solitude, seclusion, private affairs and concerns of Plaintiffs and Class Members.

WHEREFORE, Plaintiffs and Class Member in states that recognize the Tort of Intrusion Upon Seclusion (such as Illinois) are entitled to declaratory relief, damages, attorney's fees, injunctive relief and equitable relief to remedy the above described misconduct.

Count IV – Breach of Contract

100. For the sake of judicial economy, Plaintiffs incorporate all of the above paragraphs into this Count as if fully set forth.

101. Panera solicited and invited Plaintiffs and the members of the Class to buy its food and beverage products.

102. Plaintiffs and Class Members accepted Panera's offers and bought Panera's food and beverage products.

103. When Plaintiffs and Class Members purchased Panera's food and beverage products they provided their Personal Identifying Information.

104. In so doing, Plaintiffs and Class Members entered into implied contracts with Panera pursuant to which Panera agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if their data had been leaked, breached and compromised.

105. Each purchase of Panera's food and beverage products by Plaintiffs and Class Members was made pursuant to the mutually agreed-upon implied contract with Panera under which Panera agreed to safeguard and protect Plaintiffs' and Class Members' Personal Identifying Information and to timely and accurately notify them if such Personal Identifying Information was compromised, leaked or stolen.

106. Plaintiffs and Class Members would not have provided and entrusted their Personal Identifying Information to Panera in the absence of the implied contract between them and Panera.

107. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Panera.

108. Panera breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the Personal Identifying Information of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their Personal Identifying Information was compromised as a result of the data leaks, hacks and/or breaches.

109. As a direct and proximate result of Panera's breaches of the implied contracts between Panera and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described herein.

WHEREFORE, Plaintiffs and class members residing in the United States are entitled to declaratory relief, damages, attorney's fees, injunctive relief and equitable relief to remedy the above described misconduct.

Count V – Negligence

110. For the sake of judicial economy, Plaintiffs incorporate all of the above paragraphs into this Count as if fully set forth.

111. Upon accepting Plaintiffs' and Class Members' Personal Identifying Information in their respective point-of-sale systems, Reward and MyPanera apps, Panera undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard their Personal Identifying Information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so.

112. This duty included, among other things, designing, maintaining, and testing Panera security systems to ensure that Plaintiffs' and the Class Members' Personal Identifying Information was adequately secured and protected.

113. Panera further had a duty to implement processes that would detect a breach of its security system in a timely manner.

114. Panera had a duty to timely disclose to Plaintiffs and Class Members that their Personal Identifying Information had been or was reasonably believed to have been compromised.

115. Timely disclosure was appropriate so that, among other things, Plaintiffs and Class Members could take appropriate measures to avoid use of bank funds, and monitor their account information and credit reports for fraudulent activity.

116. Panera breached its duty to discover and to notify Plaintiffs and Class Members of the unauthorized access by failing to discover the security breach within reasonable time and by failing to notify Plaintiffs and Class Members of the breached and/or leaked data.

117. To date, Panera has not provided sufficient information to Plaintiffs and Class Members regarding the extent and scope of the breached and/or leaked data and continues to breach its duty to disclose the extent to the breached and/or leaked data to Plaintiffs and the Class.

118. Panera also breached its duty to Plaintiffs and Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Personal Identifying Information.

119. Furthering its negligent practices, Panera failed to provide adequate supervision and oversight of the Personal Identifying Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' Personal Identifying Information, misuse the Personal Identifying Information, and intentionally disclose it to others without consent.

120. Through Panera's acts and omissions described in this Complaint, including Panera's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' Personal Identifying Information from being foreseeably captured, accessed, disseminated, stolen, and misused, Panera unlawfully breached its

duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Personal Identifying Information during the time it was within Panera's control.

121. Further, through its failure to timely discover and provide clear notification of the data breach to consumers, Panera prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Personal Identifying Information.

122. Upon information and belief, Panera improperly and inadequately safeguarded the Personal Identifying Information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the data leak and/or breach.

123. Panera's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive Personal Identifying Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Identifying Information.

124. Panera's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Personal Identifying Information; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' Personal Identifying Information.

125. Neither Plaintiffs nor the other Class Members contributed to the data breach and/leak and subsequent misuse of their Personal Identifying Information as described in this Complaint.

126. As a direct and proximate result of Panera's negligence, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

127. As a direct and proximate result of Panera's breaches of the implied contracts between Panera and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described herein.

WHEREFORE, Plaintiffs and class members residing in the United States are entitled to declaratory relief, damages, attorney's fees, injunctive relief and equitable relief to remedy the above described misconduct.

Count VI – Right of Privacy

128. For the sake of judicial economy, Plaintiffs incorporate all of the above paragraphs into this Count as if fully set forth.

129. Under the law of each state of residence of the Plaintiffs and Class Members maintain a legally protected privacy interest in the Personal Identifying Information they provided to Panera.

130. Plaintiffs and Class Members had a reasonable expectation of privacy as to the Personal Identifying Information they provided to Panera under the circumstances of their purchases or use of Panera's Rewards of MyPanera App.

131. Panera's actions and inactions amounted to a serious invasion of the protected privacy interests of Plaintiffs and Class Members.

132. Panera's invasion of Plaintiffs and Class Members' reasonable expectation of privacy caused Plaintiffs and Class members to suffer damages.

WHEREFORE, Plaintiffs and class members residing in the United States are entitled to declaratory relief, damages, attorney's fees, injunctive relief and equitable relief to remedy the above described misconduct.

General Prayer For Relief

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Panera as follows:

A. For an Order certifying the Nationwide Class and statewide Classes as defined here, and appointing Plaintiffs and their Counsel to represent the Nationwide Class and statewide Classes;

B. For equitable relief enjoining Panera from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Personal Identifying Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiffs and Class Members;

C. For equitable relief compelling Panera to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of Personal Identifying Information compromised.

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Panera's wrongful conduct;

E. For an award of actual damages and compensatory damages, in an amount to be determined; and

F. For an award of costs of suit and attorneys' fees, to the extent allowed by law.

V. The Elements of Rule 23 Are Satisfied

133. The elements of Fed. R. Civ. P. 23 will be satisfied.

134. Excluded from each of the proposed Classes are all employees, officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Panera, including any entity in which Panera has a controlling interest, any parent

or subsidiary, or which is controlled by Panera, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Panera.

135. Also excluded are the judges and court personnel in this case and any members of their immediate families.

136. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

137. *Numerosity*. Fed. R. Civ. P. 23(a)(1). The members of the Classes are so numerous that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, Panera has acknowledged that the information of at least 10,000 customers' was made available on its website.

138. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court.

139. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control.

140. *Commonality*. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members.

141. These common questions of law and fact include, without limitation:

- a. whether Panera owed a duty of care to Plaintiffs and Class Members with respect to the security of their personal information;
- b. whether Panera took reasonable steps and measures to safeguard Plaintiffs' and Class Members' personal information;
- c. whether Panera failed to implement reasonable security procedures and practices;
- d. whether Panera violated common and statutory law by failing to promptly notify Class Members their personal information had been compromised;

- e. which security procedures and which data-breach notification procedure should Panera be required to implement as part of any injunctive relief ordered by the Court;
- f. whether Panera has an implied contractual obligation to use reasonable security measures;
- g. whether Panera has complied with any implied contractual obligation to use reasonable security measures;
- h. whether Panera's acts and omissions described herein give rise to a claim of negligence or recklessness;
- i. whether Panera knew or should have known of the security breach or leaks prior to its disclosure;
- j. whether Panera had a duty to promptly notify Plaintiffs and Class Members that their personal information was, or potentially could be, compromised;
- k. what security measures, if any, must be implemented by Panera to comply with its implied contractual obligations; and
- l. whether Panera violated state law in connection with the acts and omissions described herein.

142. *Typicality*. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Personal Identifying Information, like that of every other Class Member, was misused and/or disclosed by Panera.

143. *Adequacy of Representation*. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class.

144. Plaintiffs have retained a competent counsel who is experienced in the litigation of class actions, including consumer rights class actions.

145. Plaintiffs intend to prosecute this action vigorously.

146. Plaintiffs' claims are typical of the claims of other members of the Class and Plaintiffs have the same non-conflicting interests as the other Members of the Class.

147. The interests of the Class would be fairly and adequately represented by Plaintiffs and their counsel.

148. *Superiority of Class Action*. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable.

149. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims.

150. There will be no difficulty in the management of this action as a class action.

151. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Panera's violations of law inflicting substantial damages in the aggregate would go un-remedied.

152. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Panera has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

Plaintiffs demand a jury on all counts where a jury trial may exist.

Respectfully Submitted,
Counsel for Plaintiffs

/s/ James C. Vlahakis
James C. Vlahakis¹
Sulaiman Law Group, Ltd.
2500 South Highland Avenue, Suite 200
Lombard, IL 60148
(630) 581-5456
jvlahakis@sulaimanlaw.com

¹ <https://www.atlasconsumerlaw.com/attorney-profiles/james-c-vlahakis/>

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

ALISHA BOYKIN, KRISTEN HANSEN, TRACY MANGANO, AMY DITTBENNER, LARA SULEIMAN and DUSICA PEREZ,

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

(c) Attorneys (Firm Name, Address, and Telephone Number) James C. Vlahakis Sulaiman Law Group, Ltd. 2500 South Highland Avenue, Suite 200, Lombard, IL 60148 (630) 575-8181

DEFENDANTS

PANERA BREAD COMPANY

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
3 Federal Question (U.S. Government Not a Party)
4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

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

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER 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

VI. CAUSE OF ACTION (Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

Federal Question, 28 U.S.C. § 1331

VII. Previous Bankruptcy Matters (For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. 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

IX. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

X. This case (check one box) Is not a refiling of a previously dismissed action is a refiling of case number previously dismissed by Judge

DATE April 5 2018

SIGNATURE OF ATTORNEY OF RECORD

s:/James C. Vlahakis

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; NOTE: federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless diversity. Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. Previous Bankruptcy Matters For nature of suit 422 and 423 enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this court. Use a separate attachment if necessary.

VIII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

IX. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

X. Refiling Information. Place an "X" in one of the two boxes indicating if the case is or is not a refiling of a previously dismissed action. If it is a refiling of a previously dismissed action, insert the case number and judge.

Date and Attorney Signature. Date and sign the civil cover sheet.