UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

THE TRAVELERS INDEMNITY COMPANY OF CONNECTICUT Plaintiff	)	CASE NUMBER: : cv ( )
VS.	)	
P.F. CHANG'S CHINA BISTRO, INC. Defendant	)	OCTOBER 2, 2014

DECLARATORY JUDGMENT COMPLAINT

Plaintiff, The Travelers Indemnity Company of Connecticut ("Travelers"), for its Declaratory Judgment Complaint against the Defendant, P.F. Chang's China Bistro, Inc. ("P.F. Chang's") alleges as follows:

Nature Of This Action

1. This is an action for declaratory relief pursuant to 28 U.S.C. § 2201, *et seq.*

2. In this action, Travelers seeks a declaration that it is not obligated to defend or indemnify P.F. Chang's under Commercial General Liability insurance policies issued by Travelers to P.F. Chang's as a Named Insured in relation to litigation arising out of an alleged theft of customers' financial information.

3. More specifically, Travelers seeks a declaration there is no defense or indemnity coverage under the Travelers policies, identified in detail below, in relation to the following litigation: (a) *Daniel Lovell, Individually And On Behalf Of A Class Of Those Similarly Situated v. P.F. Chang's China Bistro, Inc.*, bearing Docket Number 2:14-cv-01152, pending in the United States District Court for the Western District of Washington, Seattle Division (the

"Lovell Lawsuit"); (b) *Lucas Kosner, Individually And On Behalf Of A Class Of Those Similarly Situated v. P.F. Chang's China Bistro, Inc.*, bearing Docket Number 1:14-cv-04923, pending in the United States District Court for the Northern District of Illinois, Eastern Division (the "Kosner Lawsuit"); and (c) *John Lewert, Individually And On Behalf Of A Class Of Those Similarly Situated v. P.F. Chang's China Bistro, Inc.*, bearing Docket Number 1:14-cv-04787, pending in the United States District Court for the Northern District of Illinois, Eastern Division (the "Lewert Lawsuit") (referred to collectively herein as the "Lawsuits").

4. P.F. Chang's provided an initial notice of claim to Travelers regarding the Lawsuits.

Jurisdiction And Venue

5. Travelers is an insurance company organized under the laws of the State of Connecticut with its principal place of business in Hartford, Connecticut. Travelers issued the subject policies, identified below, from its offices in Connecticut. The documentation relating to the Travelers policies is presently located at Travelers' Connecticut offices.

6. Upon information and belief, Defendant P.F. Chang's is a Delaware corporation with its principal place of business in Scottsdale, Arizona. P.F. Chang's conducts business in Connecticut, advertises in Connecticut, and operates multiple restaurants in Connecticut. Accordingly, this Court has personal jurisdiction over P.F. Chang's.

7. The amount in controversy exceeds $75,000 exclusive of costs and interest.

8. Jurisdiction in this Court therefore is proper under 28 U.S.C. § 1332 (a) (1) in that Travelers and P.F. Chang's are citizens of different states, and the amount in controversy exceeds $75,000.

9. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to this action occurred in this judicial district and the Court has personal jurisdiction over the Defendant, P.F. Chang's.

The Policies At Issue

10. Travelers issued Policy No. HC2E-GLSA-9355B838-TCT-13 to P.F. Chang's as a Named Insured for the policy period January 1, 2013 to January 1, 2014 (the "2013 Policy").

11. Travelers issued Policy No. HC2E-GLSA-9355B838-TCT-14 to P.F. Chang's as a Named Insured for the policy period January 1, 2014 to January 1, 2015 (the "2014 Policy"). The 2013 Policy and the 2014 Policy are referred to collectively herein as "the Policies."

12. The policy provisions relevant to this Declaratory Judgment Action are identified below. However, Travelers expressly reserves its right to rely on the Policies, in their entirety, in seeking a declaratory judgment that there is no duty to defend or indemnify P.F. Chang's under the Policies in relation to the Lawsuits. Further, Travelers reserves the right to modify and amend this Declaratory Judgment Complaint.

The Lovell Lawsuit

13. On or about July 30, 2014, Daniel Lovell filed the Lovell Lawsuit in the United States District Court for the Western District of Washington, Seattle Division. A true and accurate copy of the July 30, 2014 Complaint (the "Lovell Complaint") is attached hereto as ***Exhibit A*** and incorporated by reference. In the Lovell Lawsuit, Lovell asserts claims arising out of P.F. Chang's alleged failure to properly safeguard its customers' financial information and a data breach resulting from that alleged failure. In the Lovell Lawsuit, Lovell seeks Class Action certification and asserts claims on his own behalf and on behalf of the allegedly similarly situated Class Members.

14. The Lovell Lawsuit includes claims for negligence (Count One), breach of implied contract (Count Two), breach of fiduciary duty (Count Three), strict liability (Count Four), negligent misrepresentation (Count Five), and violations of the Arizona Deceptive Trade Practices Act (Count Six). In the prayer for relief, Lovell seeks, *inter alia*, damages, including actual, statutory and punitive damages, as well as attorney's fees, litigation costs, and interest.

15. More particularly, the Lovell Complaint includes the following pertinent allegations: P.F. Chang's failed to prevent a significant data breach that compromised its customers' personal financial data; as a result of P.F. Chang's lapses in security, criminal hackers were able to obtain access to credit and debit card data between September 18, 2013 and June 11, 2014; during this period of time, P.F. Chang's failed to disclose to its customers that its "subpar security systems placed their financial data at risk;" P.F. Chang's received notice of the breach on June 10, 2014; and P.F. Chang's confirmed the breach on June 13, 2014. (Lovell Complaint, ¶¶ 1-3, 9.) Lovell further alleges that the aggregate amount in controversy exceeds $5,000,000. (Lovell Complaint, ¶ 6.) These allegations are incorporated by reference into each Count of the Lovell Complaint.

16. The Lovell Complaint also includes allegations that P.F. Chang's likely could have prevented this data breach. (Lovell Complaint, p. 7.) In support of this position, Lovell alleges that P.F. Chang's should have been on notice to ensure its own systems were not vulnerable to a similar attack in light of prior breaches, including a recent breach involving the Target Corporation. (Lovell Complaint, ¶¶ 15-17.) Lovell further claims the "length of time that P.F. Chang's security was compromised strongly suggests that the Company was failing to comply with the Payment Card Industry Data Security Standard" (Lovell Complaint, ¶¶ 18-20), and "there is significant evidence P.F. Chang's was using outdated point-of-sale software"

(Lovell Complaint, ¶¶ 21-22). Further, Lovell alleges that had Lovell and the Class Members known P.F. Chang's did not abide by industry-standard security practices, they would have paid less for their meals or not eaten at P.F. Chang's. (Lovell Complaint, ¶¶ 4, 23.) Once again, these allegations are incorporated into each Count of the Lovell Complaint.

17. The Lovell Complaint also includes allegations that Lovell and the Class Members entered into implied contracts with P.F. Chang's under which P.F. Chang's agreed to safeguard and protect all information. (Lovell Complaint, ¶ 42.) Lovell further alleges that he and the Class Members would not have entrusted their private, confidential financial and personal information to P.F. Chang's in the absence of such an implied contract with P.F. Chang's. These allegations are incorporated into Counts Two through Six of the Lovell Complaint.

18. With regard to claimed damages, Lovell alleges: Lovell and the Class Members would have paid less for their meals or not purchased them at all had P.F. Chang's disclosed the alleged security risks; cyber-criminals now possess the personal financial information belonging to Lovell and the Class Members; and Lovell and the Class Members must replace their credit cards, update their information and add themselves to credit fraud lists, which impairs their ability to obtain additional credit. (Lovell Complaint, ¶¶ 23-24.)

19. P.F. Chang's is presently represented in the Lovell Lawsuit by attorneys from the law firm of Lewis, Brisbois, Bisgaard & Smith LLP, upon information and belief, pursuant to a separate cyber liability insurance policy that Travelers did not issue. The Policies contain a Liability Self-Funded Retentions Endorsement, Form CG D6 09 10 11, which modifies the CGL coverage part and which provides a Self-Funded Retention of $250,000 applicable to Each CGL Incident. Even if there is coverage under the Policies, which Travelers expressly denies,

Travelers does not presently have a defense obligation under the Policies because, upon information and belief, P.F. Chang's has not exhausted the Policies' Self-Funded Retention.

The Kosner Lawsuit

20. On or about June 30, 2014, Lucas Kosner filed the Kosner Lawsuit in the United States District Court for the Northern District of Illinois, Eastern Division. A true and accurate copy of the Complaint, dated June 30, 2014 (the "Kosner Complaint"), is attached hereto as ***Exhibit B*** and incorporated by reference. In the Kosner Lawsuit, Kosner asserts claims arising out of P.F. Chang's alleged failure to properly safeguard its customers' financial information, including credit and debit card information. Kosner seeks Class Action certification and filed the suit on his own behalf and on behalf of the allegedly similarly situated Class Members.

21. The Kosner Complaint includes claims for breach of implied contract (Count One), violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, as well as substantially similar laws of the Consumer Fraud Statutes (Counts Two and Three). In the prayer for relief, Kosner seeks, *inter alia*, damages, including actual, statutory and punitive damages, as well as attorney's fees, litigation costs, and interest.

22. More particularly, the Kosner Complaint includes the following pertinent allegations: P.F. Chang's received notification on June 10, 2014 from the United States Secret Service of a data breach involving the theft of customers' credit and debit card data (Kosner Complaint, ¶ 2); on June 12, 2014, P.F. Chang's confirmed the data breach, which reportedly involved approximately seven million customer credit/debit cards and began on or about September 18, 2013, almost nine months before P.F. Chang's became aware of the intrusion (Kosner Complaint, ¶ 3); and P.F. Chang's security failures enabled hackers to steal financial data and subsequently make unauthorized purchases on customers' credit, as well as debit, cards

and otherwise put the customers' financial information at a serious and ongoing risk (Kosner Complaint, ¶ 4).

23. Kosner further alleges: the security breach "was caused and enabled by [P.F. Chang's] knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information" (Kosner Complaint, ¶ 5); "P.F. Chang's grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred" (Kosner Complaint, ¶ 5); Kosner entered into an implied contract with P.F. Chang's for the adequate protection of his financial information and had his financial information exposed as a result of P.F. Chang's inadequate security (Kosner Complaint, ¶ 11); "P.F. Chang's allowed widespread and systematic theft of its customers' financial information" (Kosner Complaint, ¶ 18); and P.F. Chang's "actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customer's financial information" (Kosner Complaint, ¶ 18). These allegations are incorporated into each Count of the Kosner Complaint.

24. Further, in Count One of the Kosner Complaint, Kosner alleges that he and the Class Members entered into an implied contract with P.F. Chang's whereby P.F. Chang's became obligated to reasonably safeguard the sensitive, non-public information, and P.F. Chang's breached this implied contract. (Kosner Complaint, ¶¶ 51-54.)

25. Counts Two and Three of the Kosner Complaint include allegations that P.F. Chang's violated state and federal consumer protection laws and that the claimed injuries were caused by P.F. Chang's fraudulent and deceptive behavior, which was conducted with reckless indifference towards the rights of others. (Kosner Complaint, ¶¶ 55-85.)

26. With regard to damages, Kosner alleges, in relevant part, that P.F. Chang's deprived its costumers the full monetary value of their transactions with the company (Kosner Complaint, ¶ 30); customers have suffered actual damages, including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments and/or related bank fees charged to their accounts (Kosner Complaint, ¶ 31); customers must expend time continuing to check their credit reports (Kosner Complaint, ¶ 32); customers have suffered damages arising from costs associated with identity theft and the increased risk of identity theft caused by P.F. Chang's wrongful conduct (Kosner Complaint, ¶ 34); and customers have suffered damages based on the opportunity cost and value of time that the customers have been forced to expend to monitor their financial and bank accounts as a result of the breach (Kosner Complaint, ¶ 35). These allegations are incorporated into each Count of the Kosner Complaint.

27. P.F. Chang's is presently represented in the Kosner Lawsuit by attorneys from the law firm of Lewis, Brisbois, Bisgaard & Smith LLP, upon information and belief, pursuant to a separate cyber liability insurance policy that Travelers did not issue. The Policies contain a Liability Self-Funded Retentions Endorsement, Form CG D6 09 10 11, which modifies the CGL coverage part and which provides a Self-Funded Retention of $250,000 applicable to Each CGL Incident. Even if there is coverage under the Policies, which Travelers expressly denies, Travelers does not presently have a defense obligation under the Policies because, upon information and belief, P.F. Chang's has not exhausted the Policies' Self-Funded Retention.

The Lewert Lawsuit

28. On or about June 25, 2014, John Lewert filed the Lewert Lawsuit in the United States District Court for the Northern District of Illinois, Eastern Division. A true and accurate copy of the Complaint, dated June 25, 2014 (the "Lewert Complaint"), is attached hereto as

Exhibit C and incorporated by reference. In the Lewert Lawsuit, John Lewert asserts claims arising out of P.F. Chang's alleged failure to properly safeguard its customers' financial information, including credit and debit card information. Lewert seeks Class Action certification and files the suit on his own behalf and on behalf of the allegedly similarly situated Class Members.

29. The Lewert Lawsuit includes claims for breach of implied contract (Count One) and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, as well as substantially similar laws of the Consumer Fraud Statutes (Count Two). In the prayer for relief, the Lewert Complaint seeks, *inter alia*, damages, including actual, statutory and punitive damages, as well as attorney's fees, litigation costs, and interest.

30. More particularly, the Lewert Complaint includes the following allegations: P.F. Chang's received notification on June 10, 2014 of a data breach involving the theft of customers' credit, as well as debit, card data and verified the breach on June 12, 2014, which reportedly began in September 2013 and involved approximately seven million accounts (Lewert Complaint, ¶ 2); and P.F. Chang's security failures enabled hackers to steal financial data and subsequently make unauthorized purchases on customers' credit, as well as debit, cards and otherwise put the customers' financial information at a serious and ongoing risk (Lewert Complaint, ¶ 3).

31. Lewert further alleges that the security breach "was caused and enabled by P.F. Chang's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information" (Lewert Complaint, ¶ 4); "P.F. Chang's failed to comply with security standards and allowed their customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could

have prevented or mitigated the Security Breach that occurred" (Lewert Complaint, ¶ 4); Lewert used a debit card to make his purchase at P.F. Chang's and, as a result, entered into an implied contract with P.F. Chang's for the adequate protection of his financial information, which was exposed as a result of P.F. Chang's inadequate security (Lewert Complaint, ¶ 10); "P.F. Chang's allowed widespread and systematic theft of its customers' financial information" (Lewert Complaint, ¶ 16); and P.F. Chang's "actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information" (Lewert Complaint, ¶ 16). These allegations are incorporated into each Count of the Lewert Complaint.

32. Further, in Count One, Lewert alleges that he and the Class Members entered into an implied contract with P.F. Chang's whereby P.F. Chang's became obligated to reasonably safeguard the sensitive, non-public information, and P.F. Chang's breached this implied contract. (Lewert Complaint, ¶¶ 52-53.)

33. In Count Two, Lewert alleges that P.F. Chang's violated state and federal consumer protection laws, and that the claimed injuries were caused by P.F. Chang's fraudulent and deceptive behavior, which was conducted with reckless indifference towards the rights of others. (Lewert Complaint, ¶¶ 55-68.)

34. With regard to damages, the Lewert Complaint includes the following pertinent allegations: P.F. Chang's deprived its costumers of the full monetary value of their transactions with the company (Lewert Complaint, ¶ 32); the customers have suffered actual damages, including monetary losses arising from unauthorized bank account and/or related bank fees charged to their accounts (Lewert Complaint, ¶ 33); customers have suffered damages arising from costs associated with identity theft and the increased risk of identity theft caused by P.F.

Chang's wrongful conduct (Lewert Complaint, ¶ 34); customers must expend time continuing to check their credit reports (Lewert Complaint, ¶ 35); and customers have suffered damages based on the opportunity cost and value of time that the customers have been forced to expend to monitor their financial and bank accounts as a result of the breach (Lewert Complaint, ¶ 36). These allegations are incorporated into each Count of the Lewert Complaint.

35. P.F. Chang's is presently represented in the Lewert Lawsuit by attorneys from the law firm of Lewis, Brisbois, Bisgaard & Smith LLP, upon information and belief, pursuant to a separate cyber liability insurance policy that Travelers did not issue. The Policies contain a Liability Self-Funded Retentions Endorsement, Form CG D6 09 10 11, which modifies the CGL coverage part and which provides a Self-Funded Retention of $250,000 applicable to Each CGL Incident. Even if there is coverage under the Policies, which Travelers expressly denies, Travelers does not presently have a defense obligation under the Policies because, upon information and belief, P.F. Chang's has not exhausted the Policies' Self-Funded Retention.

First Count – Declaratory Judgment – No Duty To Defend – No Coverage Triggered Under The Policies

36. Travelers incorporates paragraphs 1-35 as if fully set forth herein.

37. The initial grant of liability coverage under the Policies' Coverage A expressly and unambiguously provides, in relevant part, as follows:

> **1. Insuring Agreement**
>
> **a.** We will pay those sums that the insured becomes legally obligated to pay as damages because of "bodily injury" or "property damage" to which this insurance applies. We will have the right and duty to defend the insured against any "suit" seeking those damages. However, we will have no duty to defend the insured against any "suit" seeking damages for "bodily injury" or "property damage" to which this insurance does not apply. . . .
>
> * * *

> **b.** This insurance applies to "bodily injury" and "property damage" only if:
>
> **(1)** The "bodily injury" or "property damage" is caused by an "occurrence" that takes place in the "coverage territory";
>
> **(2)** The "bodily injury" or "property damage" occurs during the policy period. . . .
>
> * * *

38. The Policies expressly and unambiguously define the term "occurrence" as follows: "'Occurrence' means an accident, including continuous or repeated exposure to substantially the same general harmful conditions."

39. The Policies expressly and unambiguously define the terms "bodily injury" and "property damage" as follows:

> **3.** "Bodily injury" means bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time.
>
> * * *
>
> With respect to all operations, "bodily injury" in the **DEFINITIONS** section of this insurance is amended to include mental anguish, mental injury, shock, fright, disability, humiliation, sickness or disease sustained by a person, including death resulting from any of these at any time.
>
> * * *
>
> "Property damage" means:
>
> **a.** Physical injury to tangible property, including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or
>
> **b.** Loss of use of tangible property that is not physically injured. All such loss of use shall be deemed to occur at the time of the "occurrence" that caused it.
>
> "Property damage" does not include loss of or damage to "electronic media and records".

As used in this definition, "electronic media and records" means:

a. Electronic data processing, recording or storage media such as films, tapes, discs, drums or cells;

b. Data stored on such media; or

c. Programming records for electronic data processing or electronically controlled equipment.

* * *

40. The initial grant of liability coverage under the Policies' Coverage B expressly and unambiguously provides, in relevant part, as follows:

1. Insuring Agreement

a. We will pay those sums that the insured becomes legally obligated to pay as damages because of "personal and advertising injury" to which this insurance applies. We will have the right and duty to defend the insured against any "suit" seeking those damages. However, we will have no duty to defend the insured against any "suit" seeking damages for "personal and advertising injury" to which this insurance does not apply.

* * *

b. This insurance applies to "personal and advertising injury" caused by an offense arising out of your business but only if the offense was committed in the "coverage territory" during the policy period.

* * *

41. By way of Endorsement No. CG D4 71 02 09, the Policies expressly and unambiguously define the term "personal and advertising injury" to mean "personal injury" or "advertising injury."

42. The Policies expressly and unambiguously define the terms "personal injury" and "advertising injury" as follows:

"Advertising injury":

a. Means injury, other than "personal injury", caused by one or more of the following offenses:

(1) Oral or written publication, including publication by electronic means, of material in your "advertisement" that slanders or libels a person or organization or disparages a person's or organization's goods, products or services, provided that the claim is made or the "suit" is brought by a person or organization that claims to have been slandered or libeled, or that claims to have had its goods, products or services disparaged;

(2) Oral or written publication, including publication by electronic means, of material in your "advertisement" that:

(a) Appropriates a person's name, voice, photograph or likeness;

(b) Unreasonably places a person in a false light; or

(c) Discloses information about a person's private life; or

(3) Infringement of copyright, "title" or "slogan" in your "advertisement", provided that the claim is made or the "suit" is brought by a person or organization that claims ownership of such copyright, "title" or "slogan".

b. Includes "bodily injury" caused by one or more of the offenses described in Paragraph a. above.

* * *

"Personal injury":

a. Means injury, other than "advertising injury", caused by one or more of the following offenses:

(1) False arrest, detention or imprisonment;

(2) Malicious prosecution;

(3) The wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies, provided that the wrongful eviction, wrongful entry or invasion of the right of private occupancy is committed by

or on behalf of the owner, landlord or lessor of that room, dwelling or premises;

(4) Oral or written publication, including publication by electronic means, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services, provided that the claim is made or the "suit" is brought by a person or organization that claims to have been slandered or libeled, or that claims to have had its goods, products or services disparaged; or

(5) Oral or written publication, including publication by electronic means, of material that:

(a) Appropriates a person's name, voice, photograph or likeness;

(b) Unreasonably places a person in a false light; or

(c) Discloses information about a person's private life.

b. Includes "bodily injury" caused by one or more of the offenses described in Paragraph **a.** above.

* * *

43. The Lawsuits fail to trigger coverage under the Policies because they do not allege "bodily injury" or "property damage" caused by an "occurrence," nor do they allege "advertising injury" or "personal injury" as the Policies expressly and unambiguously define those terms.

44. Travelers therefore is entitled to a declaration that it does not have a duty to defend P.F. Chang's in the pending Lawsuits.

Second Count – Declaratory Judgment – No Duty To Indemnify – No Coverage Triggered Under the Policies

45. Travelers incorporates paragraphs 1-44 as if fully set forth herein.

46. Travelers therefore is entitled to a declaration that it does not have a duty to indemnify P.F. Chang's in the pending Lawsuits.

Third Count – Declaratory Judgment – No Duty To Defend – Exclusions For Violation Of Consumer Financial Protection Laws

47. Travelers incorporates paragraphs 1-46 as if fully set forth herein.

48. The Policies contain exclusions for Violation of Consumer Financial Protection Laws, which expressly and unambiguously state that the insurance does not apply to:

> **Violation Of Consumer Financial Protection Laws**
>
> "Bodily injury" or "property damage" arising out of any actual or alleged violation of a "consumer financial protection law", or any other "bodily injury" or "property damage" alleged in any claim or "suit" that also alleges any such violation.
>
> * * *
>
> **Violation Of Consumer Financial Protection Laws**
>
> "Personal injury" or "advertising injury" arising out of any actual or alleged violation of a "consumer financial protection law", or any other "personal injury" or "advertising injury" alleged in any claim or "suit" that also alleges any such violation.
>
> * * *

49. The Policies expressly and unambiguously define the terms "consumer financial identity information" and "consumer financial protection law" as follows:

> "Consumer financial identity information" means any of the following information for a person that is used or collected for the purpose of serving as a factor in establishing such person's eligibility for personal credit, insurance or employment, or for the purpose of conducting a business transaction:
>
> **a.** Part or all of the account number, the expiration date or the balance of any credit, debit, bank or other financial account.
>
> **b.** Information bearing on a person's credit worthiness, credit standing or credit capacity.
>
> **c.** Social security number.
>
> **d.** Drivers license number.

e. Birth date.

"Consumer financial protection law" means:

a. The Fair Credit Reporting Act (FCRA) and any of its amendments, including the Fair and Accurate Credit Transactions Act (FACTA);

b. California's Song-Beverly Credit Card Act and any of its amendments; or

c. Any other law or regulation that restricts or prohibits the collection, dissemination, transmission, distribution or use of "consumer financial identity information".

* * *

50. Travelers denies that the Lawsuits trigger coverage under the Policies; however, even if the Lawsuits trigger coverage, the above-referenced express, unambiguous exclusions for Violation of Consumer Financial Protection Laws bar coverage.

51. Travelers therefore is entitled to a declaration it does not have a duty to defend P.F. Chang's in the pending Lawsuits.

Fourth Count – Declaratory Judgment – No Duty To Indemnify – Exclusions For Violation Of Consumer Financial Protection Laws

52. Travelers incorporates paragraphs 1-51 as if fully set forth herein.

53. Travelers therefore is entitled to a declaration it does not have a duty to indemnify P.F. Chang's in the pending Lawsuits.

WHEREFORE, Travelers respectfully requests a judgment against P.F Chang's as follows:

(a) Declaring that Travelers is not obligated to defend P.F Chang's as to the claims asserted against it in the Lovell Lawsuit;

(b) Declaring that Travelers is not obligated to indemnify P.F. Chang's for any amounts the underlying plaintiffs recover against P.F. Chang's in the Lovell Lawsuit, whether by judgment, settlement or otherwise;

(c) Declaring that Travelers is not obligated to defend P.F Chang's as to the claims asserted against it in the Kosner Lawsuit;

(d) Declaring that Travelers is not obligated to indemnify P.F. Chang's for any amounts the underlying plaintiffs recover against P.F. Chang's in the Kosner Lawsuit, whether by judgment, settlement or otherwise;

(e) Declaring that Travelers is not obligated to defend P.F Chang's as to the claims asserted against it in the Lewert Lawsuit;

(f) Declaring that Travelers is not obligated to indemnify P.F. Chang's for any amounts the underlying plaintiffs recover against P.F. Chang's in the Lewert Lawsuit, whether by judgment, settlement or otherwise;

(g) Declaring that Travelers does not presently have a duty to defend P.F. Chang's in the Lawsuits because P.F. Chang's has not exhausted the Policies' Self-Funded Retention;

(h) Awarding Travelers its attorneys' fees and costs in this action; and

(i) Awarding such other and further relief allowed by law and/or equity as the Court deems just and proper.

JURY DEMAND ON ALL CLAIMS AND DEFENSES SO TRIABLE

The Travelers Indemnity Company of Connecticut hereby demands a jury trial with respect to all issues so triable.

Dated at Simsbury, Connecticut on this 2nd day of October, 2014.

THE PLAINTIFF,
THE TRAVELERS INDEMNITY
COMPANY OF CONNECTICUT

By /s/ Robert L. Ciociola

Robert L. Ciociola, ct21313
Melicent B. Thompson, ct19868
Kathleen F. Adams, ct28120
Litchfield Cavo LLP
82 Hopmeadow Street, Suite 210
Simsbury, CT 06089-9694
Tel: (860) 413-2800
Fax: (860) 413-2801
ciociola@litchfieldcavo.com
thompson@litchfieldcavo.com
adamsk@litchfieldcavo.com

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

DANIEL LOVELL, individually and on behalf of a class of those similarly situated,	)	No. _____
Plaintiff,	)	CLASS ACTION COMPLAINT
v.	)	JURY TRIAL DEMANDED
P.F. CHANGS CHINA BISTRO, INC.,	)	
Defendant.	)	

Plaintiff Daniel Lovell on behalf of a class of similarly situated people (further defined below) alleges the following upon personal knowledge as to himself and his own acts and as to all other matters upon information and belief, based upon, among other things, his attorneys' investigation.

I. INTRODUCTION

1. A data breach is not an act of God. It is, almost always, the predictable and preventable result of one or more security failures by the targeted company. According to a 2014 report by the Online Trust Alliance—an industry group of leading cybersecurity experts—89% of data breaches in 2013 were preventable. Similarly, Verizon Enterprise Solution's 2014 Data Breach Investigations Report—which examined over 63,000 security incidents with the assistance of dozens of industry and government stakeholders—found that "nearly every incident involve[d] some element of human error." The Verizon report found that 92% of all attacks fell into one of nine predictable (and, thus, preventable) patterns.

2. Defendant P.F. Chang's China Bistro ("P.F. Chang's" or the "Company") failed to prevent a significant data breach that compromised its customers' personal financial data (the

"Breach"). As a result of P.F. Chang's lapses, criminal hackers were able to obtain access to credit and debit card data from customers who used their payment cards at P.F. Chang's between September 18, 2013 and June 11, 2014 (the "Relevant Period"; those who used a credit or debit card at a U.S.-based P.F. Chang's within the Relevant Period are members of the "Class").

3. During the Relevant Period, P.F. Chang's failed to disclose to the Class that its subpar security systems placed their financial data at risk. Had Class members received full disclosure of the security risks to which P.F. Chang's was exposing them, they would have paid less for their meals or not purchased them at all. Now that the Breach has occurred, Class members have been further damaged by the need to take affirmative measures to protect against fraudulent charges and other acts of identity theft.

II. PARTIES

4. Plaintiff Daniel Lovell is, and at all relevant times was, a resident of Olympia, Washington. On February 19, 2014, February 20, 2014, and May 6, 2014, Mr. Lovell ate at a P.F. Chang's location in Seattle, Washington and paid with a credit card each time. In total, Mr. Lovell spent $53.67 at P.F. Chang's over the course of his three visits. Upon information and belief, Mr. Lovell's credit card data was stolen as part of the Breach. As a result of the breach, Mr. Lovell is now forced to monitor his financial accounts for fraudulent charges and other indications of identity theft. Had Mr. Lovell known that P.F. Chang's did not abide by industry-standard cybersecurity practices, he would have paid less for his meal or not eaten at P.F. Chang's at all.

5. Defendant P.F. Chang's China Bistro is a Delaware corporation with corporate headquarters in Scottsdale, Arizona. P.F. Chang's is a wholly owned subsidiary of Centerbridge

Partners, a New-York-based private equity firm. P.F. Chang's does not franchise domestically in the United States. It directly owns all of its U.S. restaurants.

III. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Class are citizens of states different from P.F. Chang's home states, and the aggregate amount in controversy exceeds $5,000,000.

7. P.F. Chang's is subject to personal jurisdiction in this Court because it operates multiple locations in Washington and Plaintiff's claims arise, in part, from payments that he made to P.F. Chang's in Seattle, Washington.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and P.F. Chang's has caused harm to class members residing in this District.

IV. SUBSTANTIVE ALLEGATIONS

A. P.F. Chang's Customer Data Was Stolen

9. On June 10, 2014, Brian Krebs—an independent investigative reporter widely considered to be a leading cybersecurity expert—reported that "thousands of newly-stolen credit and debit cards went up for sale on rescator[.]so, an underground store best known for selling tens of millions of cards stolen in the Target breach." Krebs contacted several banks who stated that the cards offered for sale had been "previously issued to customers, and found that all had been used at P.F. Chang's locations[.]" P.F. Chang's stated, at the time, that it had not yet been able to confirm a breach but was "in communications with law enforcement authorities and banks to investigate the source."

10. On June 13, 2014, P.F. Chang's confirmed the Breach and issued the following statement:

> On Tuesday, June 10, P.F. Chang's learned of a security compromise that involves credit and debit card data reportedly stolen from some of our restaurants. Immediately, we initiated an investigation with the United States Secret Service and a team of third-party forensics experts to understand the nature and scope of the incident, and while the investigation is still ongoing, we have concluded that data has been compromised.
>
> At P.F. Chang's, the safety and security of our guests' payment information is a top priority. Therefore, we have moved to a manual credit card imprinting system for all P.F. Chang's China Bistro branded restaurants located in the continental United States. This ensures our guests can still use their credit and debit cards safely in our restaurants as our investigation continues.
>
> We have also established a dedicated public website, pfchangs.com/security, for guests to receive updates and answers to their questions.
>
> Because we are still in the preliminary stages of our investigation, we encourage our guests to be vigilant about checking their credit card and bank statements. Any suspected fraudulent activity should be immediately reported to their card company.
>
> We sincerely regret the inconvenience and concern this may cause for our guests.

11. A spokesperson for P.F. Chang's stated further that "all domestic P.F. Chang's branded restaurants in the Continental U.S. will be retaining the carbon copies [of manually imprinted cards]. P.F. Chang's is also deploying dial-up card readers to restaurants that will be plugged in via the PSTN fax line and used to process the slips."

12. On June 18, 2014, Krebs reported that Visa had sent a Compromised Account Management System ("CAMS") alert on June 17, 2014 to at least one bank stating that the bank had "many hundreds of cards exposed in a recent breach that dated back to Sept. 18, 2013. That bank had purchased more than a dozen cards sold from an underground store [that had] been exclusively selling cards stolen in the P.F. Chang's break-in, and every one of those cards was listed on the June 17 CAMS alert from Visa."

13. On July 1, 2014, P.F. Chang's issued the following statement and Frequently Asked Questions (FAQ) section:

STATEMENT FROM RICK FEDERICO
CEO OF P.F. CHANG'S

JULY 1, 2014

We continue to make progress in our investigation into the recent security compromise that affected P.F. Chang's.

The following frequently asked questions have been updated to address many of the questions or concerns you may have.

We will continue sharing important details once they have been confirmed by a team of third-party forensic experts. This website remains the best source of information on the investigation into the compromise and our ongoing response.

We look forward to welcoming you at our restaurants and appreciate your patience as the investigation continues.

1. WHAT HAPPENED?

On Tuesday, June 10, P.F. Chang's learned of a security compromise that involves credit and debit card data reportedly stolen from some of our restaurants. Immediately, we initiated an investigation with the United States Secret Service and a team of third-party forensics experts to understand the nature and scope of the incident, and have concluded that data has been compromised.

2. WHEN DID P.F. CHANG'S DISCOVER THIS INCIDENT?

The United States Secret Services alerted P.F. Chang's to this incident on June 10, 2014.

3. WHEN DID THIS INCIDENT START?

We are coordinating with the United States Secret Service on an investigation to determine when the incident started and what information is involved. To assist with these efforts, P.F. Chang's retained specialized data privacy counsel and forensics experts who are actively assisting in the investigation.

4. WHY IS THE INVESTIGATION TAKING SO LONG?

The security compromise was part of a highly sophisticated criminal operation that is being investigated by both the United States Secret Service and a team of third-party forensic experts. An investigation of this nature takes time, and while we would like to be in a position to provide further information, we can only share details that have been confirmed by the investigators.

5. WHAT INFORMATION WAS EXPOSED?

According to the United States Secret Service, credit card and debit card numbers that have been used at P.F. Chang's are involved.

6. WHAT ACTION SHOULD I TAKE?

If you suspect fraudulent activity on your credit card or debit card, we urge you to report this suspected fraudulent activity to your card company or issuing bank.

7. WHAT ACTION IS P.F. CHANG'S TAKING IN RESPONSE TO THIS INCIDENT?

P.F. Chang's continues to work with a team of third-party forensic experts to investigate this incident. P.F. Chang's is also cooperating with the United States Secret Service as they investigate. Once our investigation has determined the scope of the compromise, we will provide that information on this website.

8. IS IT SAFE FOR CUSTOMERS TO USE THEIR CREDIT CARD/DEBIT CARD?

Yes. It is safe for our guests to use their credit and debit cards in our restaurants. We are using encryption-enabled terminals to securely process credit and debit card information.

9. WHY DID YOU DECIDE TO USE MANUAL CREDIT CARD IMPRINTING DEVICES? HOW LONG WILL YOU HOLD ONTO MY SLIP FOR?

When we became aware of the security compromise, our first priority was to ensure the safety and security of our guests' payment information in our restaurants. The fastest alternative was to transition to manual imprinting devices (a.k.a. "knuckle busters") to safely process credit and debit card payments at all P.F. Chang's China Bistro branded restaurants in the continental U.S. P.F. Chang's is handling the storage and destruction of these slips according to the data protection processes required by the credit and debit card companies.

We have recently deployed additional encryption-enabled terminals to improve speed and automation in an effort to phase out the use of the "knuckle busters."

10. IF YOU ARE USING MANUAL IMPRINTING DEVICES, WHY DOES MY RECEIPT LOOK LIKE IT WAS PROCESSED ELECTRONICALLY?

> All P.F. Chang's China Bistro branded restaurants in the continental U.S. were provided with an encryption-enabled terminal to securely process credit and debit card information. Over the last week, we have deployed additional terminals to our restaurants, which has helped the speed and automation of our transactions. It has also allowed our restaurants to begin phasing out the manual credit card imprinting. In the near future, we will complete the deployment of new hardware and begin the transition back to our standard card processing system.
>
> 11. WILL P.F. CHANG'S CONTACT ME IF MY CREDIT CARD WAS INVOLVED?
>
> We are continuing to work closely with the third party forensic team and will provide information to the credit card companies to assist with efforts to identify the affected cards. The card companies can then provide this information to the issuing banks, who have the best means of directly contacting their affected credit and debit card holders. We encourage all of our guests to continue monitoring their accounts and to report any suspected fraudulent activity to their card company or issuing bank.
>
> Once the investigation has determined the scope of the compromise, we will provide that information on our dedicated website pfchangs.com/security. Please check this website for updates.
>
> 12. WHERE SHOULD I GO FOR UPDATES?
>
> We encourage you to check this website for updates. If you have additional questions, you may also call 1-877-412-7152.

B. P.F. Chang's Likely Could Have Prevented the Breach

14. For several reasons, it is highly likely that—as in most data breaches—incompetence and negligence by the target company, P.F. Chang's, caused the Breach.

15. First, the widely reported breach of Target Corporation should have put P.F. Chang's on notice to ensure that its own systems were not vulnerable to a similar attack. The Target breach was first reported in December 2013. The Target breach affected tens of millions of people, was the subject of a Congressional investigation, led to dozens of lawsuits and resulted in the resignations of Target's CEO and its Chief Information Officer.

16. The evidence suggests that the P.F. Chang's Breach was committed by the same people who committed the Target breach and that they used the same or similar methods to attack P.F. Chang's. As noted above, the stolen P.F. Chang's cards were advertised on the same underground website that sold many of the cards that were stolen in the Target breach. Moreover, it has been reported that the Target breach was accomplished by installing malicious software ("malware") known as BlackPOS on Target's point-of-sale terminals. It seems likely that the P.F. Chang's attack also targeted point-of-sale terminals because the Company's response was to stop swiping cards using its point-of-sale terminals. Matthew J. Schwartz, a cybersecurity expert and reporter for InformationWeek, echoed this conclusion in a June 17, 2014 article, writing that "[g]iven the Rescator connection detailed above, it's possible that P.F. Chang's was [like Target] also compromised using POS malware. P.F. Chang's investigators - based either on early findings or else simply prudence - seem to have come to a similar conclusion, since the restaurant chain last week stopped swiping cards using its POS terminals."

17. In a June 13, 2014 story, eWeek (a leading information technology website) reported that "Philip Casesa, director of IT/service operations for security education group (ISC)2, told eWEEK that P.F. Chang's security compromise appears to follow the same approach that attackers leveraged in the big Target breach, in which point-of-sale (POS) machines with traditionally weak security were targeted." "Large retailers maintain centralized connections to these machines for updating, and an attacker can exploit that to distribute malware efficiently and collect large swaths of magnetic stripe data from the cards," Casesa said. "Without proper detection of this malware on the retailer's part, these breaches can run almost unfettered until the attackers have enough or their exploit window is somehow closed."

18. Second, the length of time that P.F. Chang's security was compromised strongly suggests that the Company was failing to comply with the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is an industry-standard information-security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and point-of-sale cards. Among other policies and procedures, PCI DSS Requirement 10 requires organizations to "Regularly Monitor and Test Networks." This includes establishing audit logs that track access to all systems and conducting a regular review of those logs. Requirement 10.6 states that organizations must "Review logs and security events for all system components to identify anomalies or suspicious activities" and states that "Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach."

19. PCI DSS Requirement 10.6.1 elaborates on the logs that should be reviewed daily: "All security events; Logs of all system components that store, process, or transmit [cardholder data] and/or [sensitive authentication data], or that could impact the security of [cardholder data] and/or [sensitive authentication data]; Logs of all critical system components; Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)."

20. P.F. Chang's failure to detect the Breach for almost nine months suggests that it was failing to implement the daily log monitoring requirements of PCI DSS. In a June 12, 2014 statement, John Harmon, the Principal Consultant of Sword & Shield Enterprise Security stated, with respect to the P.F. Chang's breach, that "Following the PCI DSS requirements, particularly the requirement for daily log monitoring will limit your breach to one or two days, not months."

21. Third, there is significant evidence that P.F. Chang's was using outdated point-of-sale software. P.F. Chang's uses the Aloha brand of point-of-sale terminals. A July 18, 2014 story by ComputerWorld reported that "Matt Oh, a senior malware researcher with HP, recently bought a single Aloha point-of-sale terminal" and found "an eye-opening mix of default passwords, at least one security flaw and a leftover database containing the names, addresses, Social Security numbers and phone numbers of employees who had access to the system. His findings have received a fair amount of attention due to the role of such systems in high-profile data breaches at retailers including Target, Neiman Marcus and Michaels." According to the story, Oh "also found a memory-related problem known as a 'heap overflow' within a component called the Aloha Durable Messaging Service, which shuttles information between front-end and back-end systems. If exploited, the heap overflow 'could provide an attacker with full system level control of the target system'. . . ."

22. According to the ComputerWorld story, "POS systems are generally supposed to be segregated from the Internet. But restaurants often make configuration errors[.]" P.F. Chang's appears to have deliberately allowed remote access to its Aloha point-of-sale terminals. According to a "P.F. Changs Case Study" published by HotSchedules, Inc., "[a]long with the P.F. Chang's IT team, HotSchedules helped to develop a custom interface for [P.F. Chang's] Aloha POS." Using that HotSchedules software, managers can access the HotSchedules Manager portal, "anywhere, anytime, easily and securely over the web." Moreover, "staff schedules export nightly to the Aloha POS[.]" The ComputerWorld story quoted Joseph Snell, the CEO of a restaurant payment company called Viableware, who stated that P.F. Chang's used the Aloha software and that "[t]hey had a hole in their armor, and an arrow went right through it."

C. Plaintiff and the Class Have Been Harmed

23. During the Relevant Period, P.F. Chang's failed to disclose to the Class any of the security weaknesses described above. Had Class members received full disclosure of the security risks to which P.F. Chang's was exposing them, they would have paid less for their meals or not purchased them at all.

24. Plaintiff and the Class have been further harmed because, as a result of the Breach, cyber-criminals now possess their personal financial information. While credit card companies offer protection against unauthorized charges, the process is long, costly, and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impairs victims' ability to obtain additional credit. Information about Plaintiff and the other Class Members may also be used to harass or stalk them.

25. Plaintiff brings this action on behalf of himself and the following Class, pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure:

> All persons in the United States who used a debit or credit card at a P.F. Chang's restaurant between September 18, 2013 and June 11, 2014.

26. The Class excludes the officers and directors, and current or former employees, as well as immediate family members thereof, of P.F. Chang's and its parents, subsidiaries, and affiliates.

27. Plaintiff reserves the right to amend the definition of this proposed Class, including by adding subclasses.

28. The Class is so numerous that joinder of all members is impracticable. P.F. Chang's has over 210 full service restaurants in the United States and the Breach lasted for almost nine months. It is almost certain that thousands of cards were compromised.

29. There are questions of fact or law common to the Class. These questions include, but are not limited to:

a. Whether P.F. Chang's had a duty to disclose failures to comply with industry-standard cybersecurity practices;

b. Whether P.F. Chang's complied with industry-standard cybersecurity practices;

c. Whether P.F. Chang's concealed its noncompliance with industry-standard cybersecurity practices from its customers; and

d. Whether P.F. Chang's failure to comply with industry-standard cybersecurity practices caused the Breach.

30. Plaintiff's claims are typical of the Class and Plaintiff is not subject to any unique defenses.

31. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's interests do not conflict with the interests of the Class. Plaintiff has retained competent counsel experienced in class action litigation of this type. Plaintiff's counsel will fairly and adequately protect the interests of the Class.

32. Certification is appropriate under Federal Rule of Civil Procedure 23(b)(3) because questions of law or fact common to the Class predominate over any questions affecting only individual members.

33. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Individual lawsuits are economically infeasible and procedurally impracticable.

34. Plaintiff knows of no difficulty to be encountered in the management of this case that would preclude its maintenance as a class action.

V. CLAIMS ALLEGED AND RELIEF SOUGHT

A. Claims Asserted By The Class

COUNT 1
Negligence

35. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

36. P.F. Chang's owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their personal and financial information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing P.F. Chang's security systems to ensure that Plaintiff and Class member's financial information was adequately secured and protected. P.F. Chang's further had a duty to implement processes that would detect a breach of its security system in a timely manner.

37. P.F. Chang's breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff and Class members' financial data in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard their data; failing to adequately monitor the security of its point-of-sale systems; allowing unauthorized access to Plaintiff and Class members' data; and failing to recognize in a timely manner that its security had been breached.

38. P.F. Chang's failures to comply with industry standards, such as PCI DSS are evidence of P.F. Chang's negligence in failing to exercise reasonable care in safeguarding and protecting the customer data in its possession.

39. But for P.F. Chang's wrongful and negligent breach of its duties owed to Plaintiff and other Class members, their financial data would not have been compromised.

40. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of P.F. Chang's failure to exercise reasonable care in safeguarding and protecting the financial data collected from customers. P.F. Chang's knew or should have known that its systems and technologies for processing and securing customers' data had security vulnerabilities.

COUNT 2
Breach Of Implied Contract

41. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

42. When they confided their private and confidential debit card and credit card information to Defendant in order to make purchases at Defendant's restaurants, Plaintiff and Class members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect all such information.

43. Plaintiff and Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract with Defendant.

44. Defendant breached the implied contracts made with Plaintiff and Class members by failing to safeguard such information.

45. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of Defendant's breaches of these implied contracts.

COUNT 3
Breach of Fiduciary Duty

46. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

47. Plaintiff and Class members entrusted private and confidential financial and personal information to the Defendant at Defendant's request and placed trust and confidence in the Defendant in order to make payments to Defendant.

48. Defendant had the benefit of a disparity of position and control and Plaintiff and Class members placed trust and confidence in Defendant.

49. Defendant had a duty to maintain the confidentiality of the private and confidential financial and personal information, to safeguard and protect it from misuse by unauthorized persons.

50. Defendant breached its duty by failing to take necessary measures to maintain the confidentiality of Plaintiff's and Class members' private and confidential financial and personal information and to safeguard and protect it from misuse by unauthorized persons.

51. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of Defendant's breach of its duty of a confidential relationship.

COUNT 4
Strict Liability

52. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

53. Defendant failed adequately to safeguard the private and confidential financial and personal information of their customers entrusted to it in the course of purchases made with debit cards and credit cards during the Relevant Period.

54. Payment by debit or credit card increasingly is a necessity for consumers. Lack of such means of payment increasingly limits their purchase options and bargaining power. Restaurants such as P.F. Chang's are eager to accept credit cards—and pay credit card

companies handsomely for that privilege—because customers using credit cards spend more money than those paying with cash.

55. Increasing reliance on electronic means of payment and other recording of personal identity and financial data has left consumers increasingly susceptible to personal data and identity theft, the adverse consequences of which also are of increasing severity.

56. Safeguarding private and confidential data of others in their possession is solely within the control of the recipients of that data, who are best able to distribute the cost of maintaining the security of that data and the consequences of the breach of such security.

57. Plaintiff and Class members confided and entrusted their private and confidential financial and personal information to Defendant solely for the purpose of effectuating payment for purchases made from Defendant and with the expectation that Defendant would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

58. Plaintiff and Class members did not contribute in any way to the breach of Defendant's information technology systems or the compromise or theft of their private and confidential financial and personal data. Accordingly, Defendant should be held strictly liable for the loss and damage suffered by Plaintiff and Class members resulting from Defendant's failure to safeguard and maintain the confidentiality of their financial and personal data.

COUNT 5
Negligent Misrepresentation

59. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

60. P.F. Chang's had special knowledge of the methods and flaws in the methods by which it secured customer payments. Plaintiff and the Class did not have access to that information. This information was material to Plaintiff and Class members' decision to purchase

their meals at P.F. Chang's. Therefore, P.F. Chang's had a duty to disclose flaws in its security methods.

61. P.F. Chang's did not disclose to Plaintiff or to any Class member that P.F. Chang's did not abide by industry-standard cybersecurity practices—including by failing to conduct daily log monitoring—and had other deficiencies in its cybersecurity.

62. Plaintiff and the Class justifiably relied on this omission, meaning that, under conditions of full disclosure, they would have paid less for their meals or would not have purchased their meals from P.F. Chang's at all.

COUNT 6
Arizona Deceptive Trade Practices Act

63. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

64. Plaintiff, the Class and P.F. Chang's are "persons" within the meaning of Ariz. Rev. Stat. § 44-1521. The goods and services provided by P.F. Chang's to Plaintiff and the Class are "merchandise" within the meaning of Ariz. Rev. Stat. § 44-1521.

65. Plaintiff and the Class were injured by P.F. Chang's employment of deceptive acts or practices in connection with the sale of merchandise, including, among other things, uniformly failing to disclose its noncompliance with industry-standard cybersecurity practices.

66. As a direct and proximate result of P.F. Chang's deceptive acts and practices, Plaintiff and the Class overpaid for the goods and services that they received from P.F. Chang's and have been damaged thereby.

VI. RELIEF REQUESTED

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter judgment in his favor as follows:

A. Certify this matter as a class action, appoint Plaintiff's attorneys as class counsel, and issue notice to the Class;

B. Enter judgment in favor of Plaintiff and the Class against P.F. Chang's;

C. Award to Plaintiff and Class members actual, statutory, and punitive damages;

D. Award appropriate pre- and post-judgment interest;

E. Grant an award of reasonable attorney's fees and other litigation costs reasonably incurred, including expert witness fees; and

F. Award any and all other relief to which Plaintiff and the Class may be entitled.

VII. JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Dated: July 30, 2014

Respectfully submitted,

BLOCK & LEVITON LLP

By: /s/ Jason M. Leviton
Jason M. Leviton (WA #34106)
Whitney E. Street
Joel A. Fleming
Block & Leviton LLP
155 Federal Street, Suite 1303
Boston, Massachusetts 02110
Tel: (617) 398-5600
Fax: (617) 507-6020
Jason@blockesq.com
Whitney@blockesq.com
Joel@blockesq.com

Counsel for Plaintiff

EXHIBIT B

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

LUCAS KOSNER, individually and on behalf of all others similarly situated, Plaintiff, v. P.F. CHANG'S CHINA BISTRO, INC., Defendant.	No. 14-cv- **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Lucas Kosner brings this Consolidated Class Action Complaint against Defendant P.F. Chang's China Bistro, Inc. ("Defendant" or "P.F. Chang's"), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against P.F. Chang's for its failure to secure and safeguard its customers' personal financial data, including credit and debit card information.

2. On June 10, 2014, the United States Secret Service alerted Defendant to a possible data breach involving the theft of customers' credit-card and debit-card data (the "Security Breach"). To uncover further details, Defendant retained data privacy counsel and forensics experts and, on June 12, 2014, announced that while the investigation was – and as of

the date of this Complaint, is – still ongoing, it had confirmed that customers' data had indeed been compromised.

3. Reportedly, approximately 7 million customer cards were compromised by the Security Breach, which began on or around September 18, 2013, almost nine months before Defendant became aware of the intrusion, and ended on June 11, 2014, one day *after* the breach was disclosed.

4. Defendant's security failures enabled the hackers to steal financial data from within Defendant's restaurants and subsequently make unauthorized purchases on customers' credit and debit cards and otherwise put Class members' financial information at serious and ongoing risk. The hackers continue to use the information they obtained as a result of Defendant's inadequate security to exploit and injure Class members across the United States.

5. The Security Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. P.F. Chang's grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

6. P.F. Chang's failed to uncover and disclose the extent of the Security Breach and notify its affected customers of the Breach in a timely manner. P.F. Chang's failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Security Breach. Furthermore, by failing to provide adequate notice, P.F. Chang's prevented Class members from protecting themselves from the Security Breach.

7. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for breach of implied contract and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

8. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of States other than Defendant's state of citizenship.

9. This Court has personal jurisdiction over P.F. Chang's because P.F. Chang's is registered with the Illinois Secretary of State to conduct business in the State of Illinois, and does conduct substantial business in the State of Illinois, such that P.F. Chang's has significant continuous and pervasive contacts with the State of Illinois. P.F. Chang's also maintains numerous restaurants and employees in the State of Illinois, including multiple restaurants compromised in the Security Breach.

10. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2) as: a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and P.F. Chang's conducts substantial business in this District.

III. PARTIES

Plaintiff Lucas Kosner

11. Lucas Kosner is citizen of the State of Illinois and is domiciled in Lake County, Illinois. Plaintiff made purchases with his debit card at a P.F. Chang's restaurant in Cook County, Illinois on April 21, 2014. As a result, Plaintiff entered into an implied contract with P.F. Chang's for the adequate protection of his card information and had his sensitive financial information exposed as a result of Defendant's inadequate security. On June 8, 2014, four fraudulent transactions were made on the debit card Plaintiff used at P.F. Chang's: a $1.00 transaction at "facebk payment" in California; a $21.16 transaction at "godaddy.com" in Arizona; a $34.95 transaction at "www.vendosupport.com" in Switzerland; and a $4.79 transaction at "www.metin2.com" in Germany.

Defendant P.F. Chang's

12. P.F. Chang's China Bistro, Inc., is a Delaware corporation with its principal place of business in Scottsdale, Arizona. P.F. Chang's is the largest full service, casual dining Chinese restaurant chain in the United States, with 211 domestic and more than a dozen international locations.

IV. FACTUAL BACKGROUND

The Data Breach

13. Like many other restaurants, P.F. Chang's processes in-store debit and credit card payments.

14. Current reports estimate that approximately 7 million customers became victims of a data breach when their personal information was taken from Defendant's payment card

information systems through the use of malicious software.[1] The breach lasted almost nine months, from September 18, 2013 to June 11, 2014.[2]

15. The hackers who accessed this personal information have wasted no time in putting it to nefarious use. On June 17, 2014, Visa issued a Compromised Account Management System (CAMS) alert including a list of compromised payment cards purchased by an unnamed bank from a black market site that was specifically offering what the sellers claimed to be card data obtained from the P.F. Chang's breach.[3] That bank had purchased more than a dozen cards sold from the underground store and every one of those cards was listed on the June 17 CAMS alert from Visa.[4] These stolen cards have already been utilized in locations in Florida, Maryland, New Jersey, Pennsylvania, Nevada, and North Carolina,[5] and represent only a small subset of the cards compromised during the breach.

16. Due to its continuing inability to adequately safeguard the personal financial information of its customers, all of Defendant's restaurants in the continental United States have implemented manual card imprinting systems to process all customer credit and debit card transactions.[6] These systems raise their own security concerns: because there is a complete card number on the manual imprint, there could be another security breach if the imprints are not shredded, burned, pulverized, or otherwise disposed of in an appropriate manner.

17. Defendant's failure to comply with reasonable security standards provided P.F. Chang's with short-term and fleeting benefits in the form of saving on the costs of compliance,

---

[1] *See* http://krebsonsecurity.com/2014/06/p-f-changs-breach-likely-began-in-sept-2013/ (last visited June 23, 2014).
[2] *Id.*
[3] *See* http://www.tripwire.com/state-of-security/top-security-stories/p-f-changs-breach-may-have-lasted-nine-months/ (last visited June 23, 2014).
[4] *See supra,* n.2.
[5] *See* http://news.softpedia.com/news/7-Million-Cards-Likely-To-Have-Been-Stolen-in-P-F-Chang-s-Breach-447538.shtml (last visited June 23, 2014).
[6] *See* http://www.pfchangs.com/security/ (last visited June 23, 2014).

but at the expense and to the severe detriment of its own customers – including Class members here – who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

18. P.F. Chang's allowed widespread and systematic theft of its customers' financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

Security Breaches Lead to Identity Theft

19. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying information ("PII") to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[7] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

20. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve.[8] Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[9]

---

[7] *See* http:///www.gao.gov/new.items/d07737.pdf .
[8] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited June 23, 2014).
[9] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

21. A person whose PII has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [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.

22. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[10] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other PII directly on various Internet websites, making the information publicly available, just as they have done here.

The Monetary Value of Privacy Protections

23. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[11]

---

[10] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009).

[11] *The Information Marketplace: Merging and Exchanging Consumer Data*, http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (last visited June 23, 2014).

24. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[12]

25. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[13]

26. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.[14] This business has created a new market for the sale and purchase of this valuable data.[15]

27. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy

---

[12] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited June 23, 2014) ("Web's Hot New Commodity: Privacy").
[13] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited June 23, 2014).
[14] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited June 23, 2014).
[15] *See supra,* fn.9.

information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[16]

28. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use – two concerns at issue here – they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[17]

29. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII, like P.F. Chang's, has deprived that consumer of the full monetary value of the consumer's transaction with the company.

Damages Sustained By Plaintiff and the Class

30. A portion of the services purchased from P.F. Chang's by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the services purchased from P.F. Chang's.

31. Plaintiff and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts, including the fraudulent charges made on Plaintiff's debit card.

---

[16] Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited June 23, 2014); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

[17] *Id.*

32. After the breach, P.F. Chang's encouraged consumers to check their credit reports, place holds on their credit reports, and close any affected accounts. However, as explained above, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

33. To date, P.F. Chang's has not offered any form of credit monitoring or identity theft protection services to any of its affected customers. In any event, as security blogger Brian Krebs notes, "credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts – such as credit and debit cards – and they're not great at stopping new account fraud committed in your name."

34. As a result of these activities, Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendant's wrongful conduct, particularly given the incidents of actual misappropriation from Class members' financial accounts.

35. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

V. CLASS ACTION ALLEGATIONS

36. Plaintiff brings Count I, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in the United States who made an in-store purchase at a P.F. Chang's restaurant using a debit or credit card at any time from September 18, 2013 through June 11, 2014 (the "National Class").

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

37. Plaintiff brings Count II, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[18] who made an in-store purchase at a P.F. Chang's restaurant using a debit or credit card at any time from September 18, 2013 through June 11, 2014 (the "Consumer Fraud Multistate Class").

Excluded from the Consumer Fraud Multistate Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

38. In the alternative to Count II, Plaintiff brings Count III, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of the following state sub-class, defined as:

> All persons residing in the State of Illinois who made an in-store purchase at a P.F. Chang's restaurant using a debit or credit card at

[18] The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code § 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq.*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349,*et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania (73 P.S. § 201-1, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6- 101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

any time from September 18, 2013 through June 11, 2014 (the "Illinois State Class").

Excluded from the Illinois State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

39. The National Class, Consumer Fraud Multistate Class, and Illinois State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

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

41. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands to millions. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Defendant's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

42. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether P.F. Chang's failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;

b. Whether P.F. Chang's properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;

c. Whether Defendant's conduct violates the Illinois and other asserted Consumer Fraud Acts;

d. Whether Defendant's conduct constitutes breach of an implied contract; and

e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

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

44. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to P.F. Chang's that are unique to Plaintiff.

45. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and he will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

46. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for P.F. Chang's. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

47. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** P.F. Chang's has acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

48. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against P.F. Chang's, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties,

and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I
Breach of Implied Contract
(On Behalf of the National Class)

49. Plaintiff incorporates paragraphs 1-48 as if fully set forth herein.

50. Customers who intended to make purchases at Defendant's restaurants with debit or credit cards were required to provide their card's magnetic strip data for payment verification.

51. In providing such financial data, Plaintiff and the other members of the Class entered into an implied contract with P.F. Chang's whereby P.F. Chang's became obligated to reasonably safeguard Plaintiff's and the other Class members' sensitive, non-public information.

52. Plaintiff and the Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract.

53. P.F. Chang's breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

54. Plaintiff and the other Class members suffered and will continue to suffer damages including but not limited to loss of their financial information and loss of money and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
(and Substantially Similar Laws of the Consumer Fraud States)
(on Behalf of the Consumer Fraud Multistate Class)

55. Plaintiff incorporates paragraphs 1-48 as if fully set forth herein.

56. Plaintiff and the other members of the Class were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while dining at P.F. Chang's.

57. P.F. Chang's intended for Plaintiff and the other members of the Class to rely on P.F. Chang's to protect the information furnished to it in connection with their debit and credit card transactions in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

58. P.F. Chang's instead handled Plaintiff's and the other Class members' personal information in such manner that it was compromised.

59. P.F. Chang's failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

60. It was foreseeable that Defendant's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

61. P.F. Chang's benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, P.F. Chang's saved on the cost of those security measures.

62. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Defendant's deception that their financial information was secure and protected when using debit and credit cards to dine at P.F. Chang's.

63. P.F. Chang's violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other Class members' private financial information, by failing to warn diners that their information was at risk, and by

failing to discover and immediately notify affected customers of the nature and extent of the security breach.

64. Defendant's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

65. Defendant's conduct constitutes unfair acts or practices as defined in that statute because P.F. Chang's caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

66. In addition, P.F. Chang's also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

> Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. 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

67. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

68. Plaintiff and the other members have suffered injury in fact and actual damages including lost money and property as a result of Defendant's violations of 815 ILCS 505/2.

69. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

70. By this conduct, P.F. Chang's violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

COUNT III
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (In the alternative to Count II and on Behalf of the Illinois State Class)

71. Plaintiff incorporates paragraphs 1-48 as if fully set forth herein.

72. Plaintiff and the other members of the Class were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while dining at P.F. Chang's.

73. P.F. Chang's intended for Plaintiff and the other members of the Class to rely on P.F. Chang's to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

74. P.F. Chang's instead handled Plaintiff's and the other Class members' personal information in such manner that it was compromised.

75. P.F. Chang's failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

76. It was foreseeable that Defendant's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

77. P.F. Chang's benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, P.F. Chang's saved on the cost of those security measures.

78. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Defendant's deception that their financial information was secure and protected when using debit and credit cards to dine at P.F. Chang's.

79. P.F. Chang's violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs' and the other members' private financial information, by failing to warn diners that their information was at risk, and by failing to discover and immediately notify affected customers of the nature and extent of the security breach.

80. Defendant's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

81. Defendant's conduct constitutes unfair acts or practices as defined in that statute because P.F. Chang's caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

82. In addition, P.F. Chang's also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

> Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. 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

83. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

84. Plaintiff and the other Class members have suffered injury in fact and actual damages including lost money and property as a result of Defendant's violations of 815 ILCS 505/2.

85. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against P.F. Chang's, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering P.F. Chang's to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering P.F. Chang's to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

D. Ordering P.F. Chang's to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Ordering P.F. Chang's to pay statutory damages, as provided by the Illinois Consumer Fraud and Deceptive Business Practices Act and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;

F. Ordering P.F. Chang's to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;

G. Ordering P.F. Chang's to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Ordering P.F. Chang's to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Dated: June 30, 2014

Respectfully submitted,

LUCAS KOSNER, individually and on behalf of all others similarly behalf of all others similarly situated

/s/ Katrina Carroll

Katrina Carroll, Esq.
kcarroll@litedepalma.com
Kyle A. Shamberg, Esq.
kshamberg@litedepalma.com
LITE DEPALMA GREENBERG, LLC
211 W. Wacker Drive
Suite 500
Chicago, Illinois 60606
312.750.1591

Richard R. Gordon
richard.gordon@gordonlawchicago.com
Gordon Law Offices, Ltd.
211 West Wacker Drive
Suite 500
Chicago, Illinois 60606
312.332.5200
Fax: 312.236.7727

EXHIBIT C

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

JOHN LEWERT, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	No.
v.	)	**JURY TRIAL DEMANDED**
P.F. CHANG'S CHINA BISTRO, INC., a Delaware corporation,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff John Lewert ("Lewert" or "Plaintiff") brings this Class Action Complaint against Defendant P.F. Chang's China Bistro, Inc. ("Defendant" or "P.F. Chang's"), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

I. NATURE OF THE ACTION

1. This action seeks redress for P.F. Chang's failure to secure and safeguard its customers' personal financial data, including credit and debit card information.

2. On June 12, 2014, P.F. Chang's disclosed a data breach involving the theft of customers' credit-card and debit-card data with an unknown number of compromised customer accounts (the "Security Breach"). While the cause of the Security Breach is presently uncertain, P.F. Chang's claims to have learned of the compromise on June 10, 2014.[1] However, the

[1] Rick Federico, *Security Compromise Update: Statement from Rick Federico* (June 12, 2014), http://www.pfchangs.com/security/.

Security Breach likely began as far back as September of 2013 –potentially impacting ***seven million*** credit and debit card accounts.[2]

3. P.F. Chang's security failures enabled hackers to steal financial data from within P.F. Chang's systems and, on information and belief, subsequently make unauthorized purchases on customers' credit cards and otherwise put Class members' financial information at serious and ongoing risk. The hackers continue to use the information they obtained as a result of P.F. Chang's inadequate security to exploit and injure Class members across the United States.

4. The Security Breach was caused and enabled by P.F. Chang's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. P.F. Chang's failed to comply with security standards and allowed their customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

5. P.F. Chang's has also failed to disclose the extent of the Security Breach and notify its affected customers in a timely manner. P.F. Chang's failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Security Breach. By failing to provide adequate notice, P.F. Chang's prevented (and continues to prevent) Class members from protecting themselves from the Security Breach.

6. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for breach of implied contract, and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and seeks injunctive relief,

[2] Brian Krebs, *P.F. Chang's Breach Likely Began in Sept. 2013*, KrebsOnSecurity (June 14, 2014), http://krebsonsecurity.com/2014/06/p-f-changs-breach-likely-began-in-sept-2013/#more-26532.

declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

7. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of States other than P.F. Chang's State of citizenship.

8. This Court has personal jurisdiction over P.F. Chang's because P.F. Chang's is registered with the Illinois Secretary of State to conduct business in the State of Illinois, and does conduct substantial business in the State of Illinois, such that P.F. Chang's has significant continuous and pervasive contacts with the State of Illinois. P.F. Chang's also maintains numerous restaurants and employees in the State of Illinois, including multiple restaurants compromised in the Security Breach.

9. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2) as: a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and P.F. Chang's conducts substantial business in this District.

III. PARTIES

Plaintiff Lewert

10. John Lewert is a citizen of Illinois and resides in Cook County, Illinois. Lewert made purchases at a P.F. Chang's restaurant in Northbrook, Illinois on or about April 3, 2014. Lewert used a debit card to make his purchase and, as a result, entered into an implied contract

with P.F. Chang's for the adequate protection of his debit card information, and had his sensitive financial information exposed as a result of P.F. Chang's inadequate security.

Defendant P.F. Chang's

11. P.F. Chang's China Bistro, Inc. is a Delaware corporation with its principal place of business in Scottsdale, Arizona. P.F. Chang's owns and operates over 200 restaurants in the United States under its Bistro brand, as well as 170 restaurants under its Pei Wei.[3]

IV. FACTUAL BACKGROUND

The Data Breach

12. P.F. Chang's operates full service Bistro and Pei Wei restaurants, both serving Chinese-inspired cuisine. Like many other restaurants, P.F. Chang's accepts debit and credit card payments.

13. On information and belief, an untold number of consumers became the victims of a data breach when their personal information was taken from P.F. Chang's payment card information systems as a result of malicious software. According to their press release, P.F. Chang's does not know the nature of the breach or the extent of the breach, although P.F. Chang's has concluded that data has been compromised.[4] P.F. Chang's has not determined if any of its Pei Wei Asian Diner locations were compromised.

14. However, one report indicates that the breach dated back to at least September 18, 2013, and that cards stolen in the P.F. Chang's breach are being sold on the black market.[5] That

[3] *Corporate Overview*, P.F. Chang's China Bistro, Inc., http://www.pfcb.com/InvestorCorporateOverview.html (last accessed June 24, 2014).

[4] Rick Federico, *Security Compromise Update: Statement from Rick Federico* (June 12, 2014), http://www.pfchangs.com/security/.

[5] "On June 17, Visa issued a new CAMS alert to one of the banks that I worked with in reporting out the P.F. Chang's story, letting them know that they had many hundrds [sic] of cards exposed in a recent breach that dated back to Sept. 18, 2013. That bank had purchased more than a dozen cards sold from an underground store that's been exclusively selling cards stolen in the P.F. Chang's break-in, and

same report estimates that nearly 7 million cards were likely compromised as a result of the breach.

15. P.F. Chang's failure to comply with reasonable security standards provided P.F. Chang's with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of P.F. Chang's own customers – including Class members here – who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

16. P.F. Chang's allowed widespread and systematic theft of its customers' financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

Security Breaches Lead to Identity Theft

17. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[6] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

18. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history and reputation and can take time, money and patience to

---

every one of those cards was listed on the June 17 CAMS alert from Visa." *See supra*, note 2 (emphasis in original).

[6]*See* http:///www.gao.gov/new.items/d07737.pdf.

resolve.[7] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[8]

19. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [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.

20. Personal identifying information ("PII") – like P.F. Chang's customer names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action– is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[9] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, and other PII directly on various Internet websites making the information publicly available.

---

[7] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Dec. 19. 2013).

[8] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

[9] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

The Monetary Value of Privacy Protections

21. At a Federal Trade Commission ("FTC") public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[10]

22. Though Commissioner's Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[11]

23. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[12]

24. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent,

---

[10] *The Information Marketplace: Merging and Exchanging Consumer Data*, http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (last visited Dec. 20, 2013).

[11] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Dec. 20, 2013).

[12] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Dec. 20, 2013).

consumers will make a profit from the surrender of their PII.[13] This business has created a new market for the sale and purchase of this valuable data.[14]

25. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[15]

26. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website.[16]

27. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

28. In addition, members of the payment card industry ("PCI") established a Security Standards Counsel ("PCI SSC") in 2006 to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

29. The PCI DSS provides, "PCI DSS applies to all entities involved in payment card processing—including merchants."[17] P.F. Chang's is a merchant that accepts payment cards.

---

[13] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited Dec. 20, 2013).

[14] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Dec. 20, 2013).

[15] Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added) (last visited Dec. 20, 2013); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

[16] *Id.*

30. The PCI DSS requires a merchant to, among other things, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test networks.

31. On information and belief, P.F. Changs failed to comply with the PCI DSS, resulting in the security breach.

Damages Sustained By Plaintiff and the Class

32. A portion of the services purchased from P.F. Chang's by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products purchased from P.F. Chang's.

33. Members of the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals and/or related bank fees charged to their accounts.

34. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by P.F. Chang's wrongful conduct, particularly given the incidents of actual misappropriation from Class members' financial accounts, as detailed above.

35. After the breach, P.F. Chang's encouraged consumers to check their credit statements and report any fraudulent activity to their card company.[18] However, as explained

[17] *Requirements an Security Assessment Procedures, Version 3.0*, Payment Card Industry Data Security Standard, at 5 (Nov. 2013), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

[18] Rick Federico, *Security Compromise Update: Statement from Rick Federico* (June 12, 2014), http://www.pfchangs.com/security/.

above, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

36. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

V. CLASS ACTION ALLEGATIONS

37. Plaintiff brings Count I, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in the United States who made an in-store purchase at a P.F. Chang's restaurant using a debit or credit card at any time from September 18, 2013 through June 10, 2014 (the "National Class").

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

38. Plaintiff brings Count II, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[19] who made an in-store purchase at a P.F. Chang's restaurant using a

[19] The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code § 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana

> debit or credit card at any time from September 18, 2013 through June 10, 2014 (the "Consumer Fraud Multistate Class").

Excluded from the Consumer Fraud Multistate Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

39. In the alternative, Plaintiff brings Count II, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in the State of Illinois who made an in-store purchase at a P.F. Chang's restaurant using a debit or credit card at any time from September 18, 2013 through June 10, 2014 (the "Illinois State Class").

Excluded from the Illinois State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

40. The National Class, Consumer Fraud Multistate Class, and Illinois State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

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

42. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and

---

(Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq.*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349,*et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6-101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

belief, Class members number in the thousands. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from P.F. Chang's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

43. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether P.F. Chang's failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;

b. Whether P.F. Chang's properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;

c. Whether P.F. Chang's conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*;

d. Whether P.F. Chang's conduct constitutes breach of an implied contract;

e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

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

45. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through P.F. Chang's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to P.F. Chang's that are unique to Plaintiff.

46. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation; and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

47. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for P.F. Chang's. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

48. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** P.F. Chang's has acted or refused to act on grounds generally applicable to P.F. Chang's and the

other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

49. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by P.F. Chang's and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against P.F. Chang's, so it would be impracticable for Class members to individually seek redress for P.F. Chang's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I
Breach of Implied Contract
(On Behalf of the National Class)

50. Plaintiff incorporates paragraphs 1-49 as if fully set forth herein.

51. P.F. Chang's customers who intended to make in-restaurant purchases with debit or credit cards were required to provide their card's magnetic strip data for payment verification.

52. In providing such financial data, Plaintiff and the other members of the Class entered into an implied contract with P.F. Chang's whereby P.F. Chang's became obligated to reasonably safeguard Plaintiff's and the other Class members' sensitive, non-public, information.

53. P.F. Chang's breached the implied contract with P.F. Chang's and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

54. P.F. Chang's and the other Class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (and Substantially Similar Laws of the Consumer Fraud States[20]) (on Behalf of the Consumer Fraud Multistate Class or, in the alternative, the Illinois State Class)

55. Plaintiff incorporates paragraphs 1-49 as if fully set forth herein.

56. Plaintiff and the other members of the Class were deceived by P.F. Chang's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at P.F. Chang's.

57. P.F. Chang's intended for Plaintiff and the other members of the Class to rely on P.F. Chang's to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

58. P.F. Chang's instead handled Plaintiff and the other Class members' personal information in such manner that it was compromised.

59. P.F. Chang's failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

[20] The Consumer Fraud States were defined at *supra* note 19.

60. It was foreseeable that P.F. Chang's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

61. P.F. Chang's benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, P.F. Chang's saved on the cost of those security measures.

62. P.F. Chang's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on P.F. Chang's deception that their financial information was secure and protected when using debit and credit cards to shop at P.F. Chang's.[21]

63. P.F. Chang's violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other members' private financial information.

64. P.F. Chang's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

65. P.F. Chang's conduct constitutes unfair acts or practices as defined in that statute because P.F. Chang's caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

66. Plaintiff and the other members have suffered injury in fact and actual damages including lost money and property as a result of P.F. Chang's violations of 815 ILCS 505/2.

[21] The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

67. Plaintiff and the other Class members' injuries were proximately caused by P.F. Chang's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

68. By this conduct, P.F. Chang's violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against P.F. Chang's, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering P.F. Chang's to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering P.F. Chang's to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

D. Ordering P.F. Chang's to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Ordering P.F. Chang's to pay statutory damages, as provided by the Illinois Consumer Fraud and Deceptive Business Practices Act and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;

F. Ordering P.F. Chang's to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;

G. Ordering P.F. Chang's to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Ordering P.F. Chang's to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Dated: June 25, 2014

Respectfully submitted,

JOHN LEWERT, individually and on behalf of all others similarly behalf of all others similarly situated

By: */s/ Joseph J. Siprut*
One of the Attorneys for Plaintiff
And the Proposed Putative Class

Joseph J. Siprut
jsiprut@siprut.com
Gregg M. Barbakoff
gbarbakoff@siprut.com
Gregory W. Jones
gjones@siprut.com
SIPRUT PC
17 North State Street
Suite 1600
Chicago, Illinois 60602
312.236.0000
Fax: 312.267.1906

4818-5605-9675, v. 1