Tina Wolfson, CA Bar No. 174806
*twolfson@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
1016 Palm Avenue
West Hollywood, California 90069
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Cornelius P. Dukelow*, OK Bar No. 19086
*cdukelow@abingtonlaw.com*
**ABINGTON COLE + ELLERY**
320 S. Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
Telephone & Facsimile: (918) 588-3400

**Pro Hac Vice* application to be submitted

*Counsel for Plaintiff*

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

KRISTIN BAKER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CHIPOTLE MEXICAN GRILL, INC., a Delaware corporation,

Defendant.

Case No. 5:17-cv-01134

**CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

Plaintiff Kristin Baker ("Plaintiff"), by and through her counsel, brings this Class Action Complaint against Defendant Chipotle Mexican Grill, Inc. ("Defendant" or "Chipotle"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

## NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), personally identifiable information such as the cardholder's names, mailing addresses, and other personal information ("PII") (collectively, "Private Information"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their Private Information had been stolen and precisely what types of information were stolen.

2. Beginning on or about March 24, 2017, hackers utilizing malicious software accessed the point-of-sale ("POS") systems at Chipotle locations throughout the United States and stole copies of Chipotle customers' Private Information (the "Data Breach"). According to Defendant, the hackers maintained operation of the malware in Defendant's POS devices at a majority, if not all, of Chipotle locations through April 18, 2017.

3. On or about April 25, 2017, Defendant confirmed that it had allowed a massive breach of its customers' Private Information to occur, stating that the malware searched for track data including "cardholder name in addition to card number, expiration date, and internal verification code[] read from the magnetic stripe of a payment card as it was being routed through the POS device."[1]

4. Defendant's security protocols were so deficient that the Data Breach continued for over three weeks while Defendant failed to even detect it—this despite

[1] <https://www.chipotle.com/security> (last visited June 8, 2017).

widespread knowledge of the malicious software (or malware) used to perpetrate the Data Breach, which, upon information and belief, was similar to the malware used to perpetrate the earlier, notorious, and widely reported data breaches affecting retailers Target and Home Depot.

5. As of May 27, 2017, Defendant's spokesperson Chris Arnold indicated that Defendant "did not know how many payment cards or customers were affected by the breach that struck most of its roughly 2,250 restaurants for varying amounts of time between March 24 and April 18."[2] Presumably, the amount of affected customers could number in the tens of millions.

6. Defendant has acknowledged the severity of the Data Breach by advising its customers of mitigation efforts such as ordering credit reports and placing fraud alerts and security freezes on their credit reports.

7. Defendant could have prevented this Data Breach. Based upon information and belief, the malicious software used in the Data Breach was similar to the malware strains hackers used in the data breaches at Target and Home Depot. While many retailers, banks, and card companies responded to recent breaches, including the Target and Home Depot breaches, by adopting technology that helps makes transactions more secure, Defendant did not.

8. Defendant disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Private Information. On information and belief, Plaintiff's and Class members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and

[2] <http://www.nbcnews.com/business/consumer/chipotle-says-hackers-hit-most-restaurants-data-breach-n765366> (last visited June 8, 2017).

appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class members' Private Information was compromised and stolen.

9. Plaintiff brings this lawsuit individually and on behalf of all others similarly situated, alleging that Defendant violated the California Consumer Records Act, Cal. Civ. Code § 1798.80, *et seq.* (the "CRA"); breached its implied contract with Plaintiff and Class members; and violated the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL").

## PARTIES

10. Plaintiff Kristin Baker is an individual and resident of Riverside County, California. On or about March 29, 2017, Plaintiff used her debit card to make a food purchase at the Chipotle restaurant located at 8956 Trautwein Road, Suite 100, Riverside, California 92508. To date, Plaintiff has not received any notice from Defendant about the Data Breach.

11. Defendant Chipotle Mexican Grill, Inc. is a Delaware corporation headquartered in Denver, Colorado. Defendant operates restaurants throughout the United States, including the location of Plaintiff's purchase in Riverside, California.

## JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Defendant, on the other, are citizens of different states.

13. This Court has jurisdiction over Defendant because it is registered to conduct business in California, has sufficient minimum contacts in California or otherwise intentionally avails itself of the markets within California, through the promotion, marketing, and sale of food sold at its restaurants located in California, to render the exercise of jurisdiction by this Court proper and necessary.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because

a substantial part of the events and omissions giving rise to this action occurred in this District as Defendant operates restaurants within this District, Plaintiff resides here, and her purchase took place at Defendant's restaurant located within this District.

## FACTUAL BACKGROUND

### A. Chipotle and its Private Information Collection Practices

15. Defendant operates approximately 2,250 restaurants in the United States. Defendant is one of the most profitable restaurant chains in the nation, reportedly with 2014 U.S. systemwide sales of $4 billion.

16. When consumers make purchases at Defendant's restaurants using credit or debit cards, Defendant collects PCD related to that card including the cardholder name, the account number, expiration date, and card verification value (CVV). Defendant stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment.

17. Through its Privacy Policy, which is available on its website, Defendant advises consumers about the categories of Private Information it collects:

> **THE INFORMATION CHIPOTLE COLLECTS AND HOW WE USE THIS INFORMATION**
>
> Chipotle only obtains personally identifiable information such as your name, email address and payment card or other information when you provide it voluntarily. For example, personal information may be collected from you to:
>
> - respond to your comments regarding a Chipotle restaurant, our websites, or other aspects of Chipotle;
> - register you for our mailing lists or as a user of online or mobile products or services we offer, or to register you for promotions or offers conducted through our websites or mobile campaigns;
> - transmit payment information for online or mobile orders;
> - respond to job inquiries and job applications submitted by you; and
> - respond to other information submitted by you to any of our websites or through any of our mobile campaigns.
>
> This information will be used for the purposes for which you provide it. We may also use this information to communicate

> with you from time to time for other purposes, such as to create personalized promotions by combining your personal information with non personal information about you, such as the amounts and types of purchases you make or any benefits you receive through our programs.
>
> . . . .
>
> **SHARING OF PERSONAL INFORMATION**
>
> Chipotle uses its best efforts to protect your personally-identifiable information and privacy. We do not sell, transfer or disclose your personal information to any third parties other than for the limited purposes described in this policy.
>
> With your permission, we will send marketing information to you, such as promotional offers or information about new product offerings, programs or restaurant openings. If you do not want to receive this stuff, you can contact us to opt out and we will not send it to you thereafter. Also with your permission, we may occasionally send marketing information to you on behalf of one of our business partners. On our websites, in our restaurants, or elsewhere, we may ask if you want to receive marketing materials from our business partners. If you want to receive this stuff, we'll send it to you… if you don't want it, just tell us and you won't get it. But remember, Chipotle will not share your personal information with any of its business partners. We will just send a mailing, e-mail, text message or similar communication on behalf of the business partner.
>
> Chipotle sometimes contacts other companies for a variety of reasons, such as fulfilling orders, assisting with promotions, and providing technical services for our websites. These companies may have access to personal information if they need it to do their work. However, we will generally obligate these companies to use any personal information only for the purpose of performing their work.[3]

18. Thus, Defendant stores massive amounts of PII and PCD on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

[3] <https://www.chipotle.com/privacy-policy> (last visited June 8, 2017).

**B. Consumers Rely On Chipotle's Private Information Security Practices**

19. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiff would not have made her purchase at Defendant's restaurant, or would not have paid as much, had she known that Defendant does not take all necessary precautions to secure her personal and financial data. Defendant failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Defendant's restaurants.

20. Furthermore, when consumers purchase food at a national restaurant chain such as Chipotle, they assume that its data security practices and policies are state-of-the-art and that it will use part of the purchase price that consumers pay for such state-of-the-art practices. Consumers thus enter into an implied contract with Defendant that Defendant will adequately secure and protect their Private Information, and will use part of the purchase price of the food to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Defendant failed to provide reasonable security measures, thereby breaching its implied contract with Plaintiff and Class members.

**C. Stolen Private Information Is Valuable to Hackers and Thieves**

21. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it may be less protected and regulated than payment card data.

22. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[4] Similarly, in the Target data breach, in addition to PCI data pertaining to

[4] Verizon 2014 PCI Compliance Report, available at <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited June 8, 2017).

40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

23. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id*.

24. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. Unfortunately, and as will be alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as national restaurant chains, Defendant's approach at maintaining the privacy of Plaintiff's and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

**D. Chipotle Failed to Segregate PCD From PII**

25. Unlike PII data, PCD (or payment card data) is heavily regulated. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

26. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data."[5]

27. One PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code.

28. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement."[6] However, segregation is recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data."[7]

---

[5] PCI DSS v. 2 at 5 (2010) (hereafter PCI Version 2).

[6] *Id.* at 10.

[7] *See* Verizon Report at 54.

29. Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a set price.[8]

**E. The 2017 Data Breach at Chipotle**

30. Reportedly starting on March 24, 2017 and lasting until April 18, 2017, hackers gained access to the POS devices at Defendant's restaurants through the operation of malware designed to access customers' payment card data, including cardholder name, card number, expiration data, and internal verification code.

31. On or about April 25, 2017, after apparently discovering the malware and purportedly removing it from its POS systems, Defendant publicly announced the Data Breach.

32. Defendant's initial statement regarding the Data Breach lacked any detail as to the number of restaurant locations, customers, or payment cards affected by the Data Breach.

33. As of May 29, 2017, Defendant still could not confirm how many customers or payment cards have been affected by the Data Breach, but conceded that most of its 2,250 restaurants were impacted and has since posted a search tool on his website to determine the period of vulnerability for any given Chipotle location during the Data Breach.

34. Defendant has not disclosed exactly what type of PII or PCD was in fact exfiltrated in the Data Breach, instead only vaguely describing what type of payment card data is typically stored on POS systems such as the one breached.

35. Without such detailed disclosure, Plaintiff and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

36. If fraud were occurring from late March to mid-April of 2017, because hackers already had their hands on cardholder data and PII, credit card company

[8] *See, e.g.*, <https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/> (last visited June 8, 2017).

analytics and other methods (undercover investigations of the black market) would likely have discovered it before April 25, 2017. Defendant has failed to provide a cogent picture of how the Data Breach occurred and its full effects on customers' PII and PCD information.

37. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors. On information and belief, while hackers scoured Defendant's networks to find a way to access PCD, they had access to and collected the PII stored on Defendant's networks.

38. Thieves already are likely to be using the Private Information stolen from Defendant to commit actual fraud.

39. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' Private Information.

40. In this regard, the software used in the attack was a malware strain designed to siphon data from cards when they are swiped at infected POS systems. Based upon information and belief, hackers had previously utilized similar malware in other recent cyber attacks, including the retail data breaches at Target and Home Depot. While many retailers, banks, and card companies have responded to these recent breaches by adopting technology and security practices that help makes transactions and stored data more secure, Defendant did not do so.

**F. <u>This Data Breach Will Result In Identity Theft and Identify Fraud</u>**

41. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach.

42. The ramifications of Defendant's failure to keep Class members' data secure are severe.

43. The information Defendant compromised, including Plaintiff's identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[9] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

44. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[10]

45. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[11] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

46. Identity thieves can use personal information such as that of Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

47. In addition, identity thieves may get medical services using consumers'

---

[9] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* <http://www.lagunawoodsvillage.com/images/lwlagunawoods/Fighting%20back%20Against%20Identity%20Theft.pdf> (last visited June 8, 2017).

[10] FTC, Warning Signs of Identity Theft, *available at* <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited June 8, 2017).

[11] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/276> (last visited June 8, 2017) (the "2013 Identity Fraud Report").

compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

48. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[12] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

49. Annual monetary losses from identity theft are in the billions of dollars.

50. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[13]

51. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [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.[14]

52. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is

---

[12] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited June 8, 2017).

[13] *See* 2013 Identity Fraud Report.

[14] GAO, Report to Congressional Requesters, at p.33 (June 2007), *available at* <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited June 8, 2017).

incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

**G. Plaintiff and Class Members Suffered Damages**

53. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

54. Plaintiff's and Class members' Private Information is private and sensitive in nature and was left inadequately protected by Defendant. Defendant did not obtain Plaintiff's and Class members' consent to disclose their Private Information to any other person as required by applicable law and industry standards.

55. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

56. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Private Information, causing them to suffer, and continue to suffer, economic damages

and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

h. overpayments to Defendant for food purchased during the Data Breach in that a portion of the price paid by Plaintiff and Class members to Defendant was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Private Information, which Defendant did not implement and, as a result, Plaintiff and Class members did not receive what they paid for and were overcharged by Defendant;

i. the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and

j. deprivation of rights they possess under the UCL.

57. Plaintiff also purchased food she otherwise would not have purchased, or paid more than she otherwise would have paid.

58. Notwithstanding Defendant's wrongful actions and inaction and the resulting Data Breach, Defendant has not offered consumers any credit monitoring and identity theft protection services, instead merely directing customers how to obtain credit reports and implement fraud alerts and security freezes.[15] This response is insufficient because, *inter alia*, it does not address many categories of damages being sought. The cost of adequate and appropriate mitigation, such as coverage or insurance, against the loss position Defendant has placed Plaintiff and Class members in, is ascertainable and is a determination appropriate for the trier of fact.

59. Defendant's response also is insufficient because, as the GAO reported, the PII/PCD could be held by criminals and used to commit fraud after any mitigation efforts expire.

## CLASS ACTION ALLEGATIONS

60. Plaintiff seeks relief in her individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of a national class and a California class (collectively, the "Class"). The national class is initially defined as follows:

> **All persons residing in the United States whose personal and/or financial information was disclosed in the data breach affecting Chipotle in 2017 (the "National Class").**

61. The California Class is initially defined as follows:

> **All persons residing in California whose personal and/or financial information was disclosed in the data breach affecting Chipotle in 2017 (the "California Class).**

62. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs,

[15] <https://www.chipotle.com/security> (last visited June 8, 2017).

predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

63. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is in the millions.

64. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant violated the CRA by failing to implement reasonable security procedures and practices;
b. Whether Defendant violated the CRA by failing to promptly notify Class members their personal information had been compromised;
c. Whether class members may obtain an injunctive relief against Defendant under the CRA or under the UCL;
d. What security procedures and data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;
e. Whether Defendant has an implied contractual obligation to use reasonable security measures;
f. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;
g. What security measures, if any, must be implemented by Defendant to comply with its implied contractual obligations;
h. Whether Defendant violated the UCL; and
i. The nature of the relief, including equitable relief, to which Plaintiff and the Class members are entitled.

65. All members of the purposed Class are readily ascertainable. Defendant has access to addresses and other contact information for millions of members of the Class, which can be used for providing notice to many Class members.

66. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was misused and/or disclosed by Defendant.

67. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

68. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

69. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

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

## COUNT I
**For Violation of the California Customer Records Act**
**Cal. Civ. Code § 1798.80, *et seq.***
**(On Behalf of the National Class or, in the alternative, the California Class)**

71. Plaintiff incorporates all foregoing substantive allegations as if fully set

forth herein.

72. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

73. By failing to implement reasonable measures to protect the California Class's personal information, Defendant violated Civil Code § 1798.81.5.

74. In addition, by failing to promptly notify all affected Chipotle customers that their Personal Information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the Data Breach, Defendant violated Civil Code § 1798.82.

75. As a direct or proximate result of Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiff and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages as described above.

76. In addition, by violating Civil Code §§ 1798.81.5 and 1798.82, Defendant "may be enjoined" under Civil Code Section 1798.84(e).

77. Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82 also constitute unlawful acts or practices under the UCL, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

78. Plaintiff accordingly requests that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored customer data; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security

personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems; (7) ordering that Defendant purge, delete, and destroy in a reasonable secure manner customer data not necessary for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who purchase Defendant's food through the internet; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their PII/PCD to third parties, as well as the steps Defendant's customers must take to protect themselves.

79. Plaintiff further requests that the Court require Defendant to identify and notify all members of the Class who have not yet been informed of the Data Breach, and to notify affected customers of any future data breaches by email within 24 hours of Defendant's discovery of a breach or possible breach and by mail within 72 hours.

## COUNT II
## Breach of Implied Contract
## (On Behalf of the National Class or, in the alternative, the California Class)

80. Plaintiff incorporates all foregoing substantive allegations as if fully set

forth herein.

81. Defendant solicited and invited Plaintiff and Class members to purchase food at Defendant's restaurants using their credit or debit cards. Plaintiff and Class members accepted Defendant's offers and used their credit or debit cards to purchase food at Defendant's restaurants during the period of the Data Breach.

82. When Plaintiff and Class members provided their PII and PCD to Defendant to make purchases at Defendant's restaurants, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards, Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised.

83. Each purchase at a Chipotle restaurant made by Plaintiff and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Defendant under which Defendant agreed to safeguard and protect Plaintiff's and Class members' PII and PCD, including all information contained in the magnetic stripe of Plaintiff's and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

84. Plaintiff and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards, to Defendant to purchase food at Defendant's restaurants in the absence of the implied contract between them and Defendant.

85. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

86. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PCD of Plaintiff and Class members and by failing to provide timely and accurate notice to them that their PII and

PCD was compromised in and as a result of the Data Breach.

87. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described above.

**COUNT III**
**Violation of the California Unfair Competition Law**
**Cal. Bus. & Prof. Code § 17200, *et seq*.**
**(On Behalf of the National Class or, in the alternative, the California Class)**

88. Plaintiff incorporates all foregoing substantive allegations as if fully set forth herein.

89. Defendant engaged in unfair, fraudulent, and unlawful business practices in violation of the UCL.

90. Plaintiff suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

91. The acts, omissions, and conduct of Defendant as alleged constitutes a "business practice" within the meaning of the UCL.

92. Defendant violated the unlawful prong of the UCL by violating, without limitation, the CRA, as alleged above.

93. Defendant also violated the unlawful prong of the UCL by failing to honor the terms of its implied contracts with Plaintiff and Class members, as alleged above.

94. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because Defendant's acts, omissions, and conduct, as alleged herein, offended public policy and constitutes immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class members. The gravity of Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

95. Defendant's conduct also undermines California public policy—as

reflected in statutes like the California Information Practices Act, Cal. Civ. Code § 1798, *et seq.*, and the CRA concerning customer records—which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

96. By failing to disclose that it does not enlist industry standard security practices, which render Defendant's customers particularly vulnerable to data breaches, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

97. A reasonable consumer would not have purchased food at a Chipotle restaurant with a credit or debit card had she known the truth about Defendant's security procedures. By withholding material information about Defendant's security practices, Defendant was able to convince customers to provide and entrust their Private Information to Defendant. Had Plaintiff known truth about Defendant's security procedures, she would not have purchased food at Chipotle, or would not have paid as much.

98. Defendant's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendant's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendant has not—to the detriment of its customers and to competition.

99. As a result of Defendant's violations of the UCL, Plaintiff and Class members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored customer data; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing,

including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems; (7) ordering that Defendant purge, delete, and destroy in a reasonable secure manner customer data not necessary for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who purchase Defendant's food through the internet; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their PII to third parties and the theft of Defendant's source code, as well as the steps Defendant's customers must take to protect themselves.

100. As a result of Defendant's violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property, as detailed above. They purchased food they otherwise would not have purchased, or paid more for that food service than they otherwise would have paid. Plaintiff requests that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Defendant not engaged in unfair competition, including by ordering restitution of all funds that Defendant may have acquired as a result of its unfair competition.

## REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' private information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class members the type of PII and PCD compromised, and other information required under Cal. Civ. Code § 1798.82;

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

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

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury for all issues so triable under the law.

Respectfully submitted,

DATED: June 9, 2017

Tina Wolfson, CA Bar No. 174806
*twolfson@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
1016 Palm Avenue
West Hollywood, California 90069
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Cornelius P. Dukelow*, OK Bar No. 19086
*cdukelow@abingtonlaw.com*
**ABINGTON COLE + ELLERY**
320 S. Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
Telephone & Facsimile: (918) 588-3400

**Pro Hac Vice* application to be submitted

*Counsel for Plaintiff*