IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. _____

TODD GORDON,
individually and on behalf of all others similarly situated,

Plaintiff,

v.

CHIPOTLE MEXICAN GRILL, INC.,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Todd Gordon ("Plaintiff"), individually and on behalf of all others similarly situated, based on personal knowledge as to his own experiences and on investigation of counsel as to all other matters, alleges the following against Defendant Chipotle Mexican Grill, Inc. ("Chipotle" or "Defendant"):

NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all others similarly situated whose personal and non-public information, including credit card and debit card numbers, credit card and debit card expiration dates, credit and debit card security information, and other credit and debit card information (collectively, "Card Information") was compromised in a massive security breach of Defendant's computer servers beginning on or around March 24, 2017 and lasting until April 18, 2017 (the "Chipotle Data Breach").

2. As alleged herein, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for customer information, including Card Information.

3. Defendant failed to take reasonable steps to employ adequate security measures or to properly protect sensitive payment card information despite well-publicized data breaches at large national retail and restaurant chains in recent years, including Arby's, Wendy's, Noodles & Company, Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, and Kmart.

4. The Chipotle Data Breach was the inevitable result of Chipotle's inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and despite that these types of data breaches were and are occurring throughout the restaurant and retail industries, Chipotle failed to ensure that it maintained adequate data security measures, failed to implement best practices, failed to upgrade its security systems, and failed to comply with industry standards by allowing its computer and point-of-sale systems to be hacked, causing customer Card Information to be stolen.

5. Defendant exposed customers to greater damages by, upon information and belief, failing to implement chip-based card technology, otherwise known as "EMV" technology. EMV – which stands for Europay, MasterCard, and Visa – is a "global standard" for cards equipped with computer chips and technology used to authenticate chip card transactions.[1] Despite this technology's growing prominence and availability, Defendant has not implemented EMV technology in its stores, and thus, left all of the information on the

[1] http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php (last visited June 8, 2017).

magnetic stripe of cards used in its restaurant locations vulnerable to theft. In 2015, Chipotle reported that it would not upgrade its terminals to EMV technology, claiming that it would slow down customer lines.[2]

6. As a direct and proximate consequence of Defendant's negligence, a massive amount of customer information was stolen from Chipotle. An investigation is still ongoing, but upon information and belief, the Chipotle Data Breach may have compromised the Card Information of thousands of (if not more) Chipotle customers. Indeed, a spokesperson for Chipotle, Chris Arnold, has acknowledged that "most" of its 2,249 restaurants were affected by the breach in the 48 contiguous states.[3] Victims of this data breach have had their Card Information compromised, have had their privacy rights violated, have been exposed to the increased risk of fraud and identify theft (with many consumers actually having suffered incidents of fraud or identity theft), and have otherwise suffered damages.

7. Moreover, Plaintiff and Class Members have incurred and will continue to incur significant costs associated with, among other things, closing out and opening new credit or debit card accounts or ordering replacement cards and/or other losses resulting from the unauthorized use of their cards or accounts.

8. Rather than assisting consumers to deal with the fraud that has and will continue to result from this data breach, Chipotle simply tells consumers to carefully monitor their accounts. In contrast to what is and has been frequently made available to consumers in recent data breaches, Chipotle has not offered or provided any monitoring service or assistance.

---

[2] http://www.foodservicenews.net/The-FSN-Feed/September-2015/Busting-Chip-and-Pin-Upgrade-Myths/ (last accessed on June 8, 2017).

[3] http://www.nrn.com/operations/chipotle-data-breach-affected-locations-nationwide (last visited June 9, 2017); https://www.eater.com/2017/4/26/15433866/chipotle-data-breach-credit-cards (last visited June 9, 2017); https://www.thedailymeal.com/news/eat/if-you-have-been-chipotle-past-few-months-you-may-be-victim-identify-theft/053017 (last visited June 9, 2017).

9. Plaintiff and the members of the Class seek to recover damages caused by Defendant's negligence, negligence per se, breach of contract and for declaratory and injunctive relief.

PARTIES

Plaintiff

10. Plaintiff Todd Gordon is an adult residing in Laveen, Arizona. On or about March 26, 2017, Plaintiff used his American Express credit card at Chipotle's Laveen, Arizona restaurant location. Per the Chipotle website, this location was affected by the Chipotle Data Breach during that time period. Less than two months later, on or about May 10, 2017, Plaintiff's same American Express credit card was used in Miami, Florida by a fraudster, causing Plaintiff's credit card account to exceed the account limit. As a result of Plaintiff's credit card account exceeding its limit through no fault of Plaintiff's own, American Express made a report to the credit bureaus, thereby negatively affecting Plaintiff's credit score and information.

11. Prior to the May 10, 2017 fraudulent transaction, Plaintiff had not experienced credit card fraud or identity theft with respect to his American Express credit card account. In fact, Plaintiff had been recently issued a brand new credit card and credit card number under his American Express account approximately six months prior to the May 10, 2017 fraudulent transaction. Furthermore, Plaintiff has no prior history of being victimized by credit card fraud. As a result of having been victimized by the Chipotle Data Breach, Plaintiff was required to spend a significant amount of time – approximately 5-6 hours – addressing the unauthorized transactions. Had Plaintiff known that Chipotle does not adequately protect Card Information and other sensitive information, he would have never made a purchase at Chipotle using his

credit card. As a result of Chipotle's failure to adequately safeguard Plaintiff's Card Information, Plaintiff has been injured.

Defendant

12. Defendant Chipotle Mexican Grill, Inc. is a Delaware corporation with a principal executive office located at 1401 Wynkoop St., Suite 500, Denver, Colorado 80202. Chipotle operates a chain of approximately 2,249 fast-casual Chipotle restaurants throughout the United States and thirty-four international Chipotle fast-casual restaurants that serve "a focused menu of burritos, tacos, burrito bowls and salads, made using fresh, high-quality ingredients," as well as eight restaurants operating under other concepts. In 2016, Chipotle's revenues totaled approximately $3.9 billion.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendant. Defendant has sufficient minimum contacts with the state of Colorado and intentionally avails itself of the consumers and markets within the state through the promotion, marketing, and sale of its food services.

15. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because Defendant conducts substantial business in this district, is headquartered in this district, and is deemed to be a citizen of this district. A substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

FACTUAL ALLEGATIONS

16. On April 25, 2017, Defendant announced the Chipotle Data Breach when it issued the following security notice:

> We want to make our customers aware that we recently detected unauthorized activity on the network that supports payment processing for purchases made in our restaurants. We immediately began an investigation with the help of leading cyber security firms, law enforcement, and our payment processor. We believe actions we have taken have stopped the unauthorized activity, and we have implemented additional security enhancements. Our investigation is focused on card transactions in our restaurants that occurred from March 24, 2017 through April 18, 2017. . . . We anticipate providing notification to any affected customers as we get further clarity about the specific timeframes and restaurant locations that may have been affected. Consistent with good practices, consumers should closely monitor their payment card statements. If anyone sees an unauthorized charge, they should immediately notify the bank that issued the card. Payment card network rules generally state that cardholders are not responsible for such charges.

17. Chipotle stores accept customer payment cards for the purchase of food, merchandise, and food services. Upon information and belief, the large majority of Chipotle's sales during the period affected by the Chipotle Data Breach were attributable to credit and debit card transactions. At a point of sale, credit and debit cards are swiped on a terminal, and either a personal identification number is entered, or a receipt is signed to finish the transaction on behalf of the customer.

18. It is well known that customer Card Information is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including Arby's, Wendy's, Noodles & Company, Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, Kmart, and many others. Chipotle was aware of the prevalence of data breaches among retailers, especially since it

previously suffered a data beach in 2004, and acknowledged the risk of a data breach of its own, as stated in its most recent Form 10-K filed with the Securities Exchange Commission ("SEC"):

> We accept electronic payment cards for payment in our restaurants. During 2016 approximately 70% of our sales were attributable to credit and debit card transactions, and credit and debit card usage could continue to increase. A number of retailers have experienced actual or potential security breaches in which credit and debit card information may have been stolen, including a number of highly publicized incidents with well-known retailers in recent years. In August 2004, the merchant bank that processed our credit and debit card transactions informed us that we may have been the victim of a possible theft of card data. As a result, we recorded losses and related expenses totaling $4.3 million from 2004 through 2006.
>
> We may in the future become subject to additional claims for purportedly fraudulent transactions arising out of the actual or alleged theft of credit or debit card information, and we may also be subject to lawsuits or other proceedings in the future relating to these types of incidents. Proceedings related to theft of credit or debit card information may be brought by payment card providers, banks and credit unions that issue cards, cardholders (either individually or as part of a class action lawsuit) and federal and state regulators. Any such proceedings could distract our management from running our business and cause us to incur significant unplanned losses and expenses. Consumer perception of our brand could also be negatively affected by these events, which could further adversely affect our results and prospects. The liabilities resulting from any of the foregoing would likely be far greater than the losses we recorded in connection with the data breach incident in 2004.[4]

19. Despite this acknowledgment of the risk of a future data breach and the widespread publicity and industry alerts regarding the other notable data breaches, Chipotle failed to take reasonable steps to adequately protect its computer systems from being breached.

[4] Chipotle Mexican Grill, Inc., Annual Report (Form 10-K) (Feb. 7, 2017), available at https://www.sec.gov/Archives/edgar/data/1058090/000105809017000009/cmg-20161231x10k.htm (at 21) (last visited June 9, 2017).

20. Chipotle is, and at all relevant times has been, aware that the Card Information it maintains is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

21. Chipotle is, and at all relevant times has been, aware of the importance of safeguarding its customers' Card Information and of the foreseeable consequences that would occur if its data security systems were breached.

22. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure consumers' valuable data is protected.

23. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of 12 information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Defendant to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

24. The 12 requirements of the PCI DSS are: Build and Maintain a Secure Network 1) Install and maintain a firewall configuration to protect cardholder data 2) Do not use vendor-supplied defaults for system passwords and other security parameters Protect Cardholder Data 3) Protect stored cardholder data 4) Encrypt transmission of cardholder data across open, public networks Maintain a Vulnerability Management Program 5) Protect all systems against malware and regularly update anti-virus software or programs 6) Develop and maintain secure systems and applications Implement Strong Access Control Measures 7) Restrict access to cardholder

data by business need to know 8) Identify and authenticate access to system components 9) Restrict physical access to cardholder data Regularly Monitor and Test Networks 10) Track and monitor all access to network resources and cardholder data 11) Regularly test security systems and processes Maintain an Information Security Policy 12) Maintain a policy that addresses information security for all personnel.[5]

25. Furthermore, PCI DSS 3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates. Defendant was at all times fully aware of its data protection obligations for Chipotle stores in light of its participation in the payment card processing networks and their daily collection and transmission of tens of thousands of sets of Card Information.

26. Defendant knew that because Chipotle stores accepted payment cards containing sensitive financial information, customers were entitled to, and did, rely on Defendant to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

27. In addition, the payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips.

28. EMV chip technology uses embedded computer chips instead of magnetic stripes to store Card Information. Unlike magnetic stripe cards that use static data (*i.e.*, the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique

[5] PCI Security Standards Council, PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2, at 9 (May 2016), www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1472840893444 (last visited June 9, 2017).

number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen.

29. Four major credit card companies (MasterCard, Visa, Discover, and American Express) set a deadline of October 1, 2015, for businesses to transition their systems from magnetic stripe to EMV technology. Chipotle did not meet that deadline, and as noted above, specifically stated it would not transition to use EMV technology.

30. Under Card Operating Regulations, businesses accepting payment cards, but not meeting the October 1, 2015 deadline, agree to be liable for damages resulting from any data breaches.

31. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by § 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

32. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

33. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[6]

34. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

35. As noted above, Chipotle acknowledged in its SEC filings that it had at least one major prior cyber-attack in 2004. Therefore, Defendant should have been aware of the need to have adequate data security systems in place.

36. Despite its 2004 data breach, Chipotle failed to upgrade and maintain its data security systems in a meaningful way so as to prevent future breaches.

37. Had Chipotle remedied the deficiencies in its IT systems and adequately protected them, it could have prevented the Chipotle Data Breach.

38. Chipotle's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Chipotle are in stark contrast and directly conflict with the PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

39. As a result of industry warnings, industry practice, the PCI DSS, and multiple well-documented data breaches, Defendant was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

---

[6] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Nov. 2011), www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personalinformation-guide-business_0.pdf (last visited June 9, 2017).

40. Chipotle has identified that the thieves used malware to steal information from credit card readers/computers at Chipotle's locations. As cards were swiped through card readers, the malware searched for tracked data, including cardholder names, numbers, expirations dates, and card verification codes from the cards' magnetic strips.[7]

41. Defendant was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used to access POS terminals since at least 2011, and specific types of malware, including RAM scraper malware, have been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Defendant was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

42. In addition to the publicly announced data breaches described above, Defendant received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[8]

43. Despite the fact that Defendant was on notice of the very real possibility of consumer data theft associated with its security practices and that Defendant knew or should have known about the elementary infirmities associated with Chipotle's security systems, it still failed to make necessary changes to its security practices and protocols.

---

[7] http://fox59.com/2017/06/01/more-than-30-indiana-locations-affected-by-chipotle-data-breach/ (last visited June 9, 2017).

[8] *See* United States Computer Emergency Readiness Team, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), www.us-cert.gov/ ncas/alerts/TA14-212A (last accessed May 3, 2017).

44. Defendant, at all times relevant to this action, had a duty to Plaintiff and members of the Class to: (a) properly secure payment card magnetic stripe information at the point of sale and on Defendant's internal networks; (b) encrypt Card Information using industry standard methods; (c) properly use and deploy up-to-date EMV technology; (d) use available technology to defend its POS terminals from well-known methods of invasion; and (e) act reasonably to prevent the foreseeable harms to Plaintiff and the Class, which would naturally result from Card Information theft.

45. Defendant negligently allowed payment card magnetic stripe information to be compromised by failing to take reasonable steps against an obvious threat.

46. In addition, in the years leading up to the Chipotle Data Breach, and during the course of the breach itself and the investigation that followed, Chipotle failed to follow the guidelines set forth by the FTC. Indeed, Julie Conroy – research director at the research and advisory firm Aite Group – has identified that "If your data was stolen through a data breach that means you were somewhere out of compliance."[9]

47. As a result of the events detailed herein, Plaintiff and members of the Class suffered losses resulting from the Chipotle Data Breach, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Chipotle that Plaintiff and Class members would have never made had they known of Chipotle's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits and balances, and bounced transactions; harm resulting from damaged credit scores and information; and other

[9] http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited June 9, 2017).

harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

48. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

49. The information stolen from Chipotle's computers can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.[10]

50. Even if credit card companies may be responsible for some of the unauthorized transactions, consumers affected by the Chipotle Data Breach may be liable for up to $50 of fraudulent charges.[11]

51. To date, Chipotle does not appear to be taking any measures to assist affected customers other than telling them to simply do the following:

- contact the three major credit bureaus;
- contact the FTC;
- place fraud alerts on credit files; and
- place security freezes on credit files; [12] [13]

52. Chipotle's failure to adequately protect consumers' Card Information has resulted in consumers having to undertake these errands that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of sums of money, while

[10] *Id*.
[11] http://www.whec.com/news/restaurants-exposed-local-couple-chipotle-breach/4500701/ (last visited June 9, 2017).
[12] *See* https://www.engadget.com/2017/05/26/chipotle-hack-stole-credit-card-information-us-march-april/ (last visited June 9, 2017) (". . . Chipotle is not offering credit monitoring services to compromised customers.").
[13] *See* https://www.chipotle.com/security (last visited June 9, 2017).

Chipotle is not doing anything to assist those affected by the data breach. Instead, as one source identified, Chipotle is putting the burden on the consumer to discover possible fraudulent transactions.[14]

CLASS ALLEGATIONS

53. Plaintiff brings this action on his own behalf, and on behalf of the following Class pursuant to FED. R. CIV. P. 23:

> All Chipotle customers who used their credit or debit card at one of the Chipotle locations affected by the Chipotle Data Breach between March 24, 2017 and April 18, 2017.

54. Excluded from the Class are Defendant, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the definitions of the Class based on discovery and further investigation.

55. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many thousands of members who are geographically dispersed. As noted above, a spokesperson for Chipotle has acknowledged that "most" of its stores were affected by the breach.

56. **Typicality**: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Chipotle's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their data and Card Information compromised in the same way by the same conduct by Chipotle.

[14] http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited June 9, 2017).

57. **Adequacy**: Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class that they seek to represent; Plaintiff has retained counsel competent and highly experienced in class-action litigation; and Plaintiff and his counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

58. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. 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.

59. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- whether Chipotle engaged in the wrongful conduct alleged herein;
- whether Chipotle owed a duty to Plaintiff and members of the Class to adequately protect their Card Information and to provide timely and accurate notice of the data breach to Plaintiff and the Class;
- whether Chipotle breached its duty to Plaintiff and the Class by failing to provide timely and accurate notice to Plaintiff and the Class about the breach;
- whether Chipotle breached duties owed to Plaintiff and the Class by failing to provide adequate data security;
- whether Chipotle violated federal and state laws, thereby breaching its duties to Plaintiff and the Class;
- whether Chipotle knew or should have known that its computer and network systems were vulnerable to attack from hackers;
- whether Chipotle's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems, resulting in the loss of customers' Card Information;
- whether Chipotle wrongfully failed to inform Plaintiff and members of the Class that it did not maintain computer software and other security procedures sufficient to reasonably safeguard consumer financial and personal data; and whether Chipotle failed to inform Plaintiff and the Class of the data breach in a timely and accurate manner;
- whether Chipotle wrongfully waited to inform Plaintiff and Class members that their sensitive financial and personal information was exposed in the security breach;

- whether Chipotle continues to breach duties to Plaintiff and Class members and continues to fail to adequately protect sensitive Card Information and other financial information;
- whether Chipotle has sufficiently addressed, remedied, or protected Plaintiff and Class members following the data breach and has taken adequate preventive and precautionary measures to ensure the Plaintiff and Class members will not experience further harm;
- whether Plaintiff and members of the Class suffered injury as a proximate result of Chipotle's conduct or failure to act; and
- whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief, and the extend of the remedies that should be afforded to Plaintiff and the Class.

COUNT I
Negligence
(Individually and on Behalf of the Class)

60. Plaintiff realleges and incorporates all previous allegations.

61. Chipotle collected Card Information from Plaintiff and Class Members in exchange for products and services.

62. Chipotle owed a duty to Plaintiff and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Chipotle's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Chipotle's security systems to ensure that Plaintiff's and Class members' financial and personal information in Chipotle's possession was adequately protected.

63. Chipotle further owed a duty to Plaintiff and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

64. Chipotle owed a duty to Plaintiff and members of the Class to provide security consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the financial and personal information of Plaintiff and members of the Class whose confidential data Chipotle obtained and maintained.

65. Chipotle knew, or should have known, of the risks inherent in collecting and storing the financial and personal information of Plaintiff and members of the Class and of the critical importance of providing adequate security of that information.

66. Chipotle's conduct created a foreseeable risk of harm to Plaintiff and members of the Class. This conduct included but was not limited to Chipotle's failure to take the steps and opportunities to prevent and stop the data breach as described in this Complaint. Chipotle's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and Class members.

67. Chipotle acted with wanton disregard for the security of Plaintiff and Class Members' personal information. Chipotle knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Chipotle knew or should have known that hackers were attempting to access the personal information in databases such as Chipotle's.

68. Chipotle breached the duties it owed to Plaintiff and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and

practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and Class members.

69. As a direct and proximate result of Chipotle's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(Individually and on behalf of the Class)

70. Plaintiff realleges and incorporates all previous allegations.

71. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Chipotle had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' personal information.

72. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Chipotle, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Chipotle's duty.

73. Chipotle violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Chipotle's conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at an international restaurant, including, specifically, the immense damages that would result to consumers and financial institutions.

74. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

75. Chipotle had a duty to Plaintiff and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' personal information.

76. Chipotle breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' financial and personal information.

77. Chipotle's violation of §5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

78. But for Chipotle's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

79. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Chipotle's breach of its duties. Chipotle knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their personal information.

80. Had Plaintiff and Class Members known that Chipotle does not adequately protect customer Card Information, they would have never made purchases at Chipotle.

81. As a direct and proximate result of Chipotle's negligence *per se*, Plaintiff and Class Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Chipotle that Plaintiff and Class members would have never made had they known of Chipotle's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Contract
(Individually and on Behalf of the Class)

82. Plaintiff realleges and incorporates all previous allegations.

83. Plaintiff and Class Members who made purchases at Chipotle during the period in which the Chipotle Data Breach occurred had express and implied contracts with Chipotle.

84. Specifically, Plaintiff and Class Members paid money to Chipotle and, in connection with those transactions, provided Chipotle with their Card Information. In exchange, Chipotle agreed, among other things: (1) to provide food products to Plaintiff and Class Members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Card Information; and (3) to protect Plaintiff's and Class Members' personal information in compliance with federal and state laws and regulations and industry standards.

85. Protection of personal information is a material term of the contracts between Plaintiff and Class Members, on the one hand, and Chipotle, on the other hand. Had Plaintiff and Class Members known that Chipotle does not adequately protect customer Card Information, they would have never made purchases at Chipotle.

86. Chipotle did not satisfy its promises and obligations to Plaintiff and Class Members under the contracts in that it did not take reasonable measures to keep Plaintiff's and Class Members' personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

87. Chipotle materially breached its contracts with Plaintiff and Class Members by failing to implement adequate payment card and Card Information security measures.

88. Plaintiff and Class Members fully performed their obligations under their contracts with Chipotle.

89. Chipotle's failure to satisfy its obligations led directly to the successful breach of Chipotle's computer servers and stored Card Information, in which Chipotle let unauthorized parties access and exfiltrate Plaintiff's and Class Members' Card Information.

90. Chipotle breached these contracts as a result of its failure to implement security measures.

91. Also as a result of Chipotle's failure to implement the security measures, Plaintiff and Class Members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

92. Accordingly, Plaintiff and Class Members have been injured as a proximate result of Chipotle's breaches of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Unjust Enrichment
(Individually and on Behalf of the Class)

93. Plaintiff realleges and incorporates all previous allegations.

94. This claim is plead in the alternative to the above contract claim.

95. Plaintiff and Class Members conferred a monetary benefit upon Chipotle in the form of monies paid for the purchase of food services.

96. Chipotle appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Chipotle also benefited from the receipt of Plaintiff's and Class members' credit card and debit card information, as this was utilized by Chipotle to facilitate payment to it.

97. The monies for food and food services that Plaintiff and Class Members paid to Chipotle were supposed to be used by Chipotle, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

98. As a result of Chipotle's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between food services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate food services without reasonable data privacy and security practices and procedures that they received.

99. Under principals of equity and good conscience, Chipotle should not be permitted to retain the money belonging to Plaintiff and Class Members because Chipotle failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated federal, state and local laws, and industry standards.

100. Chipotle should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and data breach alleged herein.

COUNT V
Violation of the Arizona Consumer Fraud Act,
ARIZ. REV. STAT. §§44-1521, *et seq.* ("ACFA")
(Individually and on behalf of the Class)

101. Plaintiff realleges and incorporates all previous allegations.

102. This cause of action is brought pursuant to the ACFA, which provides in pertinent part:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

Id. § 44-1522.

103. Plaintiff and members of the Class are "persons" as defined by ARIZ. REV. STAT. § 44-1521(6), Chipotle provides "services" as that term is included in the definition of "merchandise" under ARIZ. REV. STAT. § 44-1521(5), and Chipotle is engaged in the "sale" of "merchandise" as defined by ARIZ. REV. STAT. § 44-1521(7).

104. Chipotle engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ACFA) in violation of the ACFA, including but not limited to the following:

- failing to maintain sufficient security to keep Plaintiff's and Class Members' sensitive Card Information being hacked and stolen;

- misrepresenting material facts to the Class, in connection with the sale of food and food services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Card Information from unauthorized disclosure, release, data breaches, and theft;

- misrepresenting material facts to the Class, in connection with sale of food and food services, by representing that Chipotle did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' Card Information;

- failing to take proper action following the data breach to enact adequate privacy and security measures and protect Class Members' Card Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

105. In addition, Chipotle's failure to disclose that its computer systems were not well-protected – including Chipotle's failure to disclose that, despite the general trend of a shift to chip technology for point of sale transactions, Chipotle had not made this transition – and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Chipotle knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary, foreseeable and reasonable expectations concerning the security of their Card Information on Chipotle's computer servers.

106. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Chipotle's offering of food and food services and incorporating Plaintiff's and Class members' Card Information on its computer servers, in violation of the AFCA.

107. Chipotle also engaged in unfair acts and practices, in connection with the sale of services by failing to maintain the privacy and security of Class Members' personal information,

in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

108. Chipotle's wrongful practices occurred in the course of trade or commerce.

109. Chipotle's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Chipotle that applied to all Class members and were repeated continuously before and after Chipotle obtained sensitive Card Information and other information from Plaintiff and Class members. All Class members have been adversely affected by Chipotle's conduct and the public was and is at risk as a result thereof.

110. As a result of Chipotle's wrongful conduct, Plaintiff and Class members were injured in that they never would have allowed their sensitive Card Information – the value of which Plaintiff and Class members no long have control – to be provided to Chipotle if they had been told or knew that Chipotle failed to maintain sufficient security to keep such data from being hacked and taken by others.

111. Chipotle's unfair and/or deceptive conduct proximately caused Plaintiff's and Class members' injuries because, had Chipotle maintained customer Card Information with adequate security, Plaintiff and the Class members would not have lost it.

112. As a direct and proximate result of Chipotle's conduct, Plaintiff and Class Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Chipotle that Plaintiff and Class members would have never made had they known of Chipotle's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of

unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

113. Plaintiff and the Class seek actual damages, compensatory, punitive damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the AFCA.

PRAYER FOR RELIEF

Plaintiff, on behalf of himself and the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiff as Class representative and his counsel as Class counsel.

B. Award Plaintiff and the Class appropriate monetary relief, including actual damages, restitution, and disgorgement.

C. Award Plaintiff and the Class equitable, injunctive and declaratory relief as may be appropriate. Plaintiff, on behalf of the Class, seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information and extend credit monitoring services and services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

D. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiff and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

Dated: June 9, 2017

Respectfully submitted,

Benjamin F. Johns
Andrew W. Ferich
Jessica L. Titler
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
awf@chimicles.com
jlt@chimicles.com

Counsel for Plaintiff and the Putative Class