UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

ALCOA COMMUNITY FEDERAL CREDIT UNION, individually and on behalf of all others similarly situated, Plaintiff, v. CHIPOTLE MEXICAN GRILL, INC., Defendant.	Case No. **Complaint - Class Action** DEMAND FOR JURY TRIAL

Plaintiff Alcoa Community Federal Credit Union ("Plaintiff"), on behalf of itself and all others similarly situated, alleges the following against Defendant Chipotle Mexican Grill, Inc. ("Chipotle" or "Defendant") and states the following:

INTRODUCTION

1. This is a class action on behalf of credit unions, banks, and other financial institutions that suffered injury as a result of a security breach beginning on or around March 24, 2017, to the present, that compromised the names, credit and debit card numbers, card expiration dates, card verification values ("CVVs"), and other credit and debit card information (collectively, "Payment Card Data") of customers of nationwide locations of Defendant's restaurants (hereinafter, the "Chipotle Data Breach").

2. The Chipotle Data Breach has forced Plaintiff and other financial institutions to: (a) cancel or reissue any credit and debit cards affected by the Chipotle Data Breach; (b) close any deposit, transaction, checking, or other accounts affected by the Chipotle Data Breach,

including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) open or reopen any deposit, transaction, checking, or other accounts affected by the Chipotle Data Breach; (d) refund or credit any cardholder for the cost of any unauthorized transaction relating to the Chipotle Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; (f) increase fraud monitoring efforts; and (g) reissue cards compromised by the Chipotle Data Breach.

3. As alleged herein, the injuries to Plaintiff and the Class (defined below) were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for customer information, including credit and debit card data and personally identifying information. Defendant failed to take reasonable steps to employ adequate security measures despite well-publicized data breaches at large, national retail and restaurant chains in recent months, including Arby's, Wendy's, Noodles & Company, Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, and Kmart.

4. Despite having knowledge that such data breaches were occurring throughout the restaurant and retail industry, Defendant failed to properly protect sensitive payment card information.

5. 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 cyber breaches involving payment card networks and systems, Chipotle systematically failed to ensure that it maintained adequate data security measures, failed to implement best practices, failed to upgrade security systems, and failed to comply with industry standards by

allowing its computer and point-of-sale ("POS") systems to be hacked, causing financial institutions' payment card and customer information to be stolen.

6. Defendant also failed to mitigate the damage of a potential data breach by 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. While Visa implemented minimum EMV Chip Card and Terminal Requirements in October 2015, Defendant has not implemented EMV technology in its stores, and thus, left vulnerable to theft all of the information on the magnetic stripe of cards used in its restaurant locations, in a way it has been repeatedly warned about. In 2015, Chipotle reported that it would not upgrade its terminals to EMV technology, claiming that it would slow down customer lines.[1]

7. As a direct and proximate consequence of Defendant's negligence, a vast amount of customer information was stolen from Chipotle's computer network. Though an investigation is still ongoing, it appears that hundreds of thousands of Defendant's customers at locations nationwide have had their credit and debit numbers compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Moreover, Plaintiff and members of the Class have incurred and will continue to incur significant costs associated with, among other things, notifying their customers of issues related to the Chipotle Data Breach, closing out and opening new customer accounts, reissuing customers' cards, and/or refunding customers' losses resulting from the unauthorized use of their accounts.

[1] *See* www.foodservicenews.net/The-FSN-Feed/September-2015/Busting-Chip-and-Pin-Upgrade-Myths (last accessed on May 23, 2017).

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

PARTIES

9. Plaintiff Alcoa Community Federal Credit Union is a not-for-profit financial cooperative with its principal place of business in Benton, Arkansas. As a result of the Chipotle Data Breach, Plaintiff has suffered, and continues to suffer, injuries, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

10. 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 fast-casual restaurants that serve "a focused menu of burritos, tacos, burrito bowls and salads, made using fresh, high-quality ingredients." As of March 31, 2017, Chipotle operates approximately 2,249 restaurants throughout the United States, as well as 34 international locations, and 8 restaurants in operation in other non-Chipotle concepts. In 2016, Chipotle's revenues totaled approximately $3.9 billion dollars.

JURISDICTION AND VENUE

11. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, many of which are citizens of a different state than Defendant. Defendant Chipotle is a citizen of Delaware, where it is incorporated, and Colorado, where its principal place of business is located.

12. The District of Colorado has personal jurisdiction over Defendant because Defendant is found within this District and conducts substantial business in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. §1391, because Defendant resides in this judicial district, regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

FACTUAL BACKGROUND

A. Background on Electronic Debit and Credit Card Transactions and Requirements for Securing Data

14. Plaintiff and the members of the Class are financial institutions that issue payment cards[2] to their customers.

15. Chipotle stores accept customer payment cards for the purchase of goods and services. In fact, as discussed below, Chipotle acknowledges that 70% of its sales were attributable to credit and debit card transactions. At a point of sale, credit and debit cards are swiped on a POS terminal, and either a personal identification number (or some other confirmation number) is entered, or a receipt is signed to finish the transaction on behalf of the customer.

16. It is well known that customer Payment Card Data 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

[2] These cards include, for example, credit or debit cards branded with the Visa or MasterCard logo.

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:

> 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.[3]

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.

17. A basic description of the various steps necessary to execute a credit/debit card transaction is as follows: (1) after the credit/debit card is swiped, the merchant (*e.g.*, Chipotle) uses one of several payment processing networks (*e.g.*, Visa or MasterCard) to transmit a request

[3] 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).

for authorization to the institution that issued the payment card (*e.g.*, Plaintiff); (2) the issuing institution authorizes the payment, and the merchant electronically forwards a receipt of the transaction to another financial institution known as the "acquiring bank," which contracts with the merchant to process credit and debit card transactions on the merchant's behalf; (3) the acquiring bank forwards the funds to the merchant to satisfy the transaction, and is then reimbursed by the issuing financial institution (*e.g.*, Plaintiff); and (4) finally, the issuing institution posts the debit or credit transaction to its customer's account.

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

19. Chipotle is, and at all relevant times has been, aware of the importance of safeguarding its customers' Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, specifically including the significant costs that would be imposed on issuers, such as the Plaintiff and members of the Class, and others. In its notice relating to the Chipotle Data Breach, Chipotle notes that "[i]f anyone sees an unauthorized charge, they should immediately notify the bank that issued the card."[4]

20. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, it is unsurprising that 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.

[4] Security Notice, Chipotle Mexican Grill, Inc., Notice of Data Security Incident (last updated April 25, 2017), www.chipotle.com/security (last accessed May 23, 2017).

21. 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.

22. 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]

23. 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 Payment Card Data.

24. Furthermore, Defendant knew that because Chipotle stores accepted payment cards containing sensitive financial information, customers and financial institutions, such as Plaintiff, 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.

25. In addition, the payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store Payment Card Data. Unlike magnetic stripe cards that use static data (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

[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=14728 40893444 (last accessed May 23, 2017).

again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen.

26. The payment card industry (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 because it would, so Chipotle claimed, slow down customer lines.

27. 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.

28. 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.

29. 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.

30. 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]

31. 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.

B. The Chipotle Data Breach: the Result of Lax Security Standards

32. 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. Because our investigation is continuing, complete findings are not available and it is too early to provide further details on the investigation. 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

[6] Federal Trade Commission, Protecting *Personal Information: A Guide for Business* (Nov. 2011), https://www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personal-information-guide-business_0.pdf (last accessed May 23, 2017).

notify the bank that issued the card. Payment card network rules generally state that cardholders are not responsible for such charges.[7]

33. In its own filings with the United States Securities and Exchange Commission, Chipotle acknowledged that it had at least one major prior cyber-attack in 2004, and therefore should have been aware of the need to have adequate data security systems in place. Specifically, in 2004, Chipotle recorded charges of $4 million to establish a reserve for claims seeking reimbursement for fraudulent credit and debit card charges, in addition to $1.5 million of additional expenses. Chipotle only learned of this cyber-attack after having been notified by the merchant bank that processed Chipotle's credit and debit card transactions. In this 2004 data breach, hackers stole "Track 2" data from Chipotle's systems, which includes the customer's name, card number, card expiration date, and card verification number. Chipotle further explained that in the 2004 data breach, the internet gateways on Defendant's computers in some stores may not have been fully secure at all times.[8]

34. Despite its 2004 data breach, Chipotle quite obviously failed to upgrade its data security systems in a meaningful way so as to prevent future breaches.

35. The deficiencies in Chipotle's security system include a lack of elementary security measures, which even the most inexperienced IT professional, could identify as problematic.

---

[7] www.chipotle.com/security.

[8] http://ir.chipotle.com/phoenix.zhtml?c=194775&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTM4NTU2MzAmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d (last accessed on May 23, 2017).

36. Had Chipotle remedied the deficiencies in its IT systems, it could have prevented the Chipotle Data Breach. In fact, the *Online Trust Alliance*, a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, in its 2014 annual report, estimated that 740 million records were stolen in 2013, and that 89% of data breaches occurring in that year were avoidable.

37. The security flaws outlined above, along with many others, were explicitly highlighted by Visa as early as 2009, when it issued a Data Security Alert describing the threat of RAM scraper malware.[9] The report instructs companies to "secure remote access connectivity," "implement secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (*i.e.*, segregate networks), "actively monitor logs of network components, including intrusion detection systems and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration." *Id*.

38. In addition to ignoring explicit warnings from Visa, Chipotle's security flaws also 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 Payment Card Industry Data Security Standard and requirements three and five of the 12 PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

[9] *Visa Data Security Alert* (Nov. 6, 2009), http://go.mercurypay.com/go/visa/targeted-hospitality-sector-vulnerabilities-110609.pdf (last accessed Nov. 30, 2016).

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.

40. 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.

41. In particular, several major and well-publicized breaches of other retailers provided Chipotle with advance warning that its POS systems would make attractive targets to hackers, and that Chipotle should take steps to secure and monitor its POS systems to prevent a breach.

42. For example, at the end of 2013, hackers infiltrated the POS network of Target Corporation and stole the credit and debit card information of approximately 40 million Target customers. That data breach received extensive publicity because it represented one of the largest data breaches ever at that time. It was reported that the hackers accessed Target's POS systems through credentials obtained from a third-party vendor, which were then used to hack the POS systems and capture Payment Card Data as a credit or debit card was scanned in the store. This data was then exfiltrated from Target's servers and sold on the internet.

43. Shortly thereafter, hackers infiltrated the network of Neiman Marcus Group, LLC with malware. Approximately 350,000 customers had their debit and credit card information stolen as a result.

44. In January of 2014, Michaels Stores, Inc. revealed that it experienced a data breach ultimately affecting three million of its customers.

45. In March of 2014, Sally Beauty Supply admitted to a data breach affecting at least 25,000 individuals.

46. In June of 2014, PF Chang's Chinese Bistro confirmed that 33 of its restaurant locations in the United States had data breaches and its customers' confidential information had been compromised.

47. In September of 2014, Home Depot confirmed that its POS system was hacked and the information of approximately 56 million Home Depot customers was stolen. Like Target, it was widely reported that hackers had installed malware directly onto Home Depot's POS systems to capture Payment Card Data at POS terminals.

48. In October 2014, Kmart Corporation announced that it, too, had been the target of malware installed on its POS system by hackers.

49. In addition to these publicly announced data breaches, 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.[10]

50. Despite the fact that Defendant was put on notice of the very real possibility of consumer data theft associated with its security practices, and despite the fact that Defendant knew or, at the very least, 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.

51. Defendant knew that failing to protect customer card data would cause harm to the card-issuing institutions, such as Plaintiff and the Class, because the issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

52. Indeed, Defendant's public statements to customers after the data breach plainly indicate that Defendant believes that card-issuing institutions should be responsible for fraudulent charges on cardholder accounts resulting from the data breach. Chipotle has made no overtures to the card-issuing institutions that are left to pay for damages as a result of the breach.

53. 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 Payment Card Data 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

[10] *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 23, 2017).

prevent the foreseeable harms to Plaintiff and the Class, which would naturally result from Payment Card Data theft.

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

55. 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. Furthermore, by failing to have reasonable data security measures in place, Chipotle engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

56. As a result of the events detailed herein, Plaintiff and members of the Class have been and continue to be forced to protect their customers and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

57. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class, all of which were proximately caused by Defendant's negligence. As a result of the events detailed herein, Plaintiff and members of the Class suffered losses resulting from the Chipotle Data Breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their customers.

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

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23. The proposed Class is defined as:

> All Financial Institutions − including, but not limited to, banks and credit unions − in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card-issuing services, whose customers made purchases from Chipotle stores from March 1, 2017 to the present (the "Class").

60. Excluded from the Class are Defendant and its subsidiaries, franchises, and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

61. Plaintiff is a member of the Class it seeks to represent.

62. The Class is so numerous that joinder of all members is impracticable.

63. The members of the Class are readily ascertainable.

64. Plaintiff's claims are typical of the claims of all members of the Class.

65. The conduct of Defendant has caused injury to Plaintiff and members of the Class in substantially the same ways.

66. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendant.

67. Plaintiff will fairly and adequately represent the interests of the Class.

68. Defendant has acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

69. Plaintiff is represented by experienced counsel, who are qualified to litigate this case.

70. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

71. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members; these questions include, without limitation:

a) whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b) whether the conduct of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

c) whether Defendant's actions were negligent;

d) whether Defendant owed a duty to Plaintiff and the Class;

e) whether the harm to Plaintiff and the Class was foreseeable;

f) whether Plaintiff and members of the Class are entitled to injunctive relief; and

g) whether Plaintiff and members of the Class are entitled to damages, and the measure of such damages.

CHOICE OF LAW

72. Chipotle's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Colorado and the tortious and deceptive acts complained of occurred in, and radiated from, Colorado.

73. The key wrongdoing at issue in this litigation (Chipotle's failure to employ adequate data security measures) emanated from Chipotle's headquarters in Colorado.

74. Chipotle's principle executive offices, as well as POS system and IT personnel, operate out of, and are located at, Chipotle's headquarters in Colorado.

75. Colorado, which seeks to protect the rights and interests of Colorado and other U.S. businesses against a company doing business in Colorado, has a greater interest in the claims of Plaintiff and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

76. Application of Colorado law to a nationwide Class, with respect to Plaintiff's and the Class members' claims, is neither arbitrary nor fundamentally unfair, because Colorado has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiff and the nationwide Class.

77. The location where Plaintiff was injured was fortuitous and Chipotle could not have foreseen where the injury would take place, as Chipotle did not know which financial institutions its customers used and the location of these institutions' headquarters, or principal places of business, at the time of the breach.

COUNT ONE
NEGLIGENCE

78. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

79. Defendant owed – and continues to owe – a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

80. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

81. Chipotle has a common law duty to prevent the foreseeable risk of harm to others, including the Plaintiff and the Class. It was certainly foreseeable to Chipotle that injury would result from a failure to use reasonable measures to protect Payment Card Data. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of Chipotle customers; thieves would use Payment Card Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

82. Chipotle assumed the duty to use reasonable security measures as a result of its conduct.

83. Chipotle's duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Chipotle. The FTC publications and data

security breach orders described above further form the basis of Chipotle's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Chipotle.

84. Defendant breached its duties by: (1) allowing a third-party intrusion into their computer systems; (2) failing to protect against such an intrusion; (3) failing to maintain updated EMV card systems, updated POS terminals, and secure systems and software necessary to prevent such an intrusion; and (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a large scale.

85. Defendant knew or should have known of the risk that its POS terminals could be infiltrated using methods similar or identical to those previously used against major retailers in recent months and years.

86. Defendant knew or should have known that its failure to take reasonable measures to protect its POS terminals against obvious risks would result in harm to Plaintiff and the Class.

87. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT TWO
NEGLIGENCE *PER SE*

88. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

89. 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.

90. 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.

91. Chipotle's violation of §5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

92. Plaintiff and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses. Moreover, many of the Class members are credit unions, which are organized as cooperatives, whose members are consumers.

93. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 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.

94. As a direct and proximate result of Chipotle's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and

reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT THREE
DECLARATORY AND INJUNCTIVE RELIEF

95. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

96. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

97. An actual controversy has arisen in the wake of the Chipotle Data Breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiff alleges that Chipotle's data security measures were inadequate and remain inadequate. Chipotle will likely deny these allegations. Furthermore, Plaintiff continues to suffer injury as additional fraudulent charges are being made on payment cards issued to Chipotle customers.

98. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Chipotle continues to owe a legal duty to secure its customers' personal and financial information – specifically including information pertaining to

credit and debit cards used by Chipotle customers – and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

(b) Chipotle continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

(c) Chipotle's ongoing breaches of its legal duty continue to cause harm to Plaintiff and the Class.

99. The Court also should issue corresponding injunctive relief requiring Chipotle to employ adequate security protocols, consistent with industry standards, to protect its Payment Card Data. Specifically, this injunction should, among other things, direct Chipotle to:

(a) utilize industry standard encryption to encrypt the transmission of cardholder data at the point of sale and at all other times;

(b) implement encryption keys in accordance with industry standards;

(c) implement EMV technology;

(d) engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

(e) audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

(f) regularly test its systems for security vulnerabilities, consistent with industry standards;

(g) comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

(h) install all upgrades recommended by manufacturers of security software and firewalls used by Chipotle.

100. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Chipotle. The risk of another such breach is real, immediate, and substantial. Indeed, Chipotle is a recidivist, having already sustained a data breach in 2004. If another breach at Chipotle occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and it will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable, and reputational damage.

101. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to Chipotle, if an injunction is issued. Among other things, if another massive data breach occurs at Chipotle, Plaintiff and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Chipotle of complying with an injunction, by employing reasonable data security measures, is relatively minimal and Chipotle has a pre-existing legal obligation to employ such measures.

102. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Chipotle, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. this action be certified as a class action, pursuant to Fed. R. Civ. P. 23, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. monetary damages;

C. injunctive relief;

D. reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. costs;

F. pre- and post-judgment interest; and

G. such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

DATED: May 26, 2017

Respectfully submitted,

/s/ *Karen S. Halbert*

Karen S. Halbert
Michael L. Roberts
Jana K. Law
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223
Telephone: (501) 821-5575

Fax: (501) 821-4474
karenhalbert@robertslawfirm.us
mikeroberts@robertslawfirm.us
janalaw@robertslawfirm.us

Attorneys for Plaintiff and Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on May 26, 2017, a copy of the foregoing was filed electronically and served by mail on anyone unable to accept electronic filing. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on May 26, 2017.

/s/ *Karen S. Halbert*
Karen S. Halbert
Michael L. Roberts
Jana K. Law
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223
Telephone: (501) 821-5575
Fax: (501) 821-4474
karenhalbert@robertslawfirm.us
mikeroberts@robertslawfirm.us
janalaw@robertslawfirm.us

Attorneys for Plaintiff and Proposed Class