IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No.

GREG LAWSON and JUDY CONARD, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CHIPOTLE MEXICAN GRILL, INC.,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Greg Lawson and Judy Conard ("Plaintiffs"), individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Chipotle Mexican Grill, Inc. ("Chipotle" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiffs bring this class action case against Chipotle for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information ("PII") which Chipotle collected at the time Plaintiffs and putative class members made purchases at restaurants owned and operated by Chipotle (collectively, "Customer Data"), and for failing to provide timely, accurate, and adequate notice to

Plaintiffs and other putative class members that their Customer Data had been stolen and precisely what types of information were stolen.

2. On April 25, 2017, Chipotle announced that Customer Data had been stolen from payment card transactions in locations across the country from March 24, 2017 through April 18, 2017 (the "Data Breach").

3. Chipotle posted the following notification on its website:

> Chipotle Mexican Grill, Inc. (Chipotle) is providing further information about the payment card security incident that Chipotle previously reported on April 25, 2017. The information comes at the completion of an investigation that involved leading cyber security firms, law enforcement, and the payment card networks.
>
> The investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Chipotle restaurants between March 24, 2017 and April 18, 2017. The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS device. There is no indication that other customer information was affected … . Not all locations were involved, and the specific time frames vary by location … .
>
> During the investigation we removed the malware, and we continue to work with cyber security firms to evaluate ways to enhance our security measures. In addition, we continue to support law enforcement's investigation and are working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring.[1]

4. According to publicly available information, the Data Breach affected "most" Chipotle restaurants and Pizzeria Locale restaurants, also owned and operated by Chipotle, located in all 48 contiguous states in the United States.[2]

[1] https://www.chipotle.com/security (last visited August 16, 2017).
[2] Jonathan Maze, *Chipotle Data Breach Affected Locations Nationwide*, Nation's Restaurant News (May 26, 2017) (citing a statement by Chipotle company spokesman that "[m]ost but not all locations may have been involved."), available at http://www.nrn.com/operations/chipotle-data-breach-affected-locations-nationwide (last visited August 1, 2017).

5. This Customer Data was compromised due to Chipotle's acts and omissions and its failure to properly protect the Customer Data.

6. Chipotle could have and should have prevented this Data Breach. Data breaches at other retail and restaurant establishments in the last few years have been the result of malware installed on POS systems. While many retailers, restaurants, banks, and other companies have responded to recent breaches by adopting technology that helps make transactions more secure, Chipotle did not.

7. The Data Breach was the inevitable result of Chipotle's inadequate approach to data security. The deficiencies in Chipotle's data security were so significant that the malware installed by the hackers remained undetected and intact for months.

8. Chipotle disregarded the rights of Plaintiffs and putative class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from happening, and failing to disclosure to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Customer Data.

9. As a result of the Chipotle Data Breach, Customer Data of Plaintiffs and putative class members has been exposed to criminals for misuse and has been misused.

10. As a direct and proximate consequence of Defendant's conduct as stated above, vast amounts of Customer Data were 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.

11. Plaintiffs retain a significant interest in ensuring that their Customer Data, which remains in the possession of Chipotle, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose Customer Data was stolen as a result of the Chipotle Data Breach. Plaintiffs assert claims against Chipotle for violations of the Colorado Consumer Protection Act ("CCPA"), breach of implied contract, and negligence.

12. Plaintiffs, on behalf of themselves and similarly situated consumers, seek to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the data breach and resulting injury, restitution, disgorgement, reasonable costs, and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members, 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. According to publicly available information, the Data Breach affected the Customer Data of patrons of most Chipotle and Pizzeria Locale restaurants located throughout the United States.

14. This Court has personal jurisdiction over Defendant because Chipotle maintains its principal place of business in Colorado, regularly conducts substantial business in Colorado, and has sufficient minimum contacts in Colorado. Defendant intentionally avails itself of this jurisdiction by marketing and selling products and services from Colorado to millions of consumers nationwide.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District, regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

PARTIES

16. Plaintiff Greg Lawson is a resident of the state of Missouri. On or around March 28, 2017, Plaintiff Greg Lawson visited Chipotle restaurant No. 0669 located at 5107 Belt Highway in St. Joseph, Missouri, and purchased food items using his debit card. This debit card is the primary card Mr. Lawson uses for daily expenditures because of the cash-back rewards benefit. Within a few weeks of this visit, Mr. Lawson was contacted by the issuing bank and advised that his debit card had been compromised as a result of the Chipotle Data Breach. The bank informed Mr. Lawson that it would be closing the account, opening a new account, and re-issuing a new debit card. Because Mr. Lawson had upcoming travel plans, he paid $45 to have the new debit card expedited to him. Unfortunately, despite the attempt to expedite and the money expenditure, a new card did not arrive before he left town. As such, Mr. Lawson did not have his debit card to use for his travel expenses as he planned. Additionally, as a result of the Data Breach, Mr. Lawson was required to spend time communicating with his bank regarding his compromised card, account transfer, and replacement card.

17. Plaintiff Greg Lawson would not have used his debit card to make purchases at Chipotle — indeed, he would not have shopped at Chipotle at all during the period of the Data Breach — had Chipotle told him that it lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

18. Plaintiff Judy Conard is a resident of the State of California. On or around April 11, 2017, and April 12, 2017, Plaintiff Conard visited a Chipotle restaurant located at 2517 Fair Oaks

Blvd. in Sacramento, California, and purchased food items using her Visa credit card. This credit card is the primary card Ms. Conard uses for daily expenditures because of the rewards benefit. On April 22, 2017, Plaintiff Conard received a call from her bank seeking approval for a $1,300 charge from Barcelona, Spain. Determining that Ms. Conard's credit card had been compromised, her bank closed the card account and re-issued a new credit card. Ms. Conard was required to spend time communicating with her bank regarding her compromised card and replacement card. She spent time contacting businesses to notify them and provide the information for her new card for established automatic payments linked to her credit card. While awaiting a replacement card, Ms. Conard had to use cash and other credit cards; accordingly, she lost the opportunity to accrue points for purchases that is a feature of her credit card. Because of the fraud experienced as a result of her credit card being compromised in the Data Breach, Ms. Conard has contracted for identity theft monitoring services through LifeLock at an annual cost of $131.93.

19. Plaintiff Judy Conard would not have used her credit card to make purchases at Chipotle — indeed, she would not have shopped at Chipotle at all during the period of the Data Breach — had Chipotle told her that it lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

20. Plaintiffs suffered actual injury from having their Customer Data compromised and stolen in and as a result of the Data Breach.

21. Plaintiffs suffered actual injury and damages in paying money to and purchasing products from Chipotle during the Data Breach that they would not have suffered and paid had Chipotle disclosed that it lacked computer systems and data security practices adequate to safeguard customers' Customer Data.

22. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Customer Data, a form of intangible property that Plaintiffs entrusted to Chipotle for the purpose of purchasing its products, which was compromised in and as a result of the Data Breach.

23. Also, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Customer Data being placed in the hands of criminals who have already misused such information stolen in the Data Breach via sale of Plaintiffs' and putative class members' Customer Data on the Internet black market, as evidenced by the compromise of Plaintiff Craig Lawson's debit card and Plaintiff Judy Conard's credit card. Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Chipotle, is protected and safeguarded from future breaches.

24. Defendant Chipotle Mexican Grill, Inc. is a Delaware corporation with a principal executive office located at 1401 Wynkoop St., Suite 500, Denver, Colorado 80202.

25. Chipotle operates a chain of fast-casual restaurants under the Chipotle name that serve "a focused menu of burritos, tacos, burrito bowls and salads, made using fresh, high-quality ingredients." Chipotle operates approximately 2,249 restaurants throughout the United States. Defendant Chipotle also owns and operates a quick-serve pizza restaurant chain, Pizzeria Locale. In 2016, Defendant Chipotle's revenues totaled approximately $3.9 billion.

26. Chipotle restaurants accept payment for their goods and services through a POS system, through which customers swipe credit and debit cards to pay.

STATEMENT OF FACTS

A. Chipotle and Its Customer Data Collection Practices

27. Chipotle and Pizzeria Locale restaurants accept customer payment cards for the purchase of goods and services. In fact, Chipotle has acknowledged that approximately 70% of its sales are attributable to credit and debit card transactions.

28. When Chipotle customers pay using credit or debit cards, Chipotle collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Chipotle stores the Customer Data in its POS system and transmits this information to a third party for completion of the payment.

29. At all relevant times, Chipotle was well-aware, or reasonably should have been aware, that the Customer Data it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

30. It is well-known that customer PCD is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurant chains nationwide. Within the last two years, massive data breaches of PCD have plagued the restaurant industry, including national restaurant chains such as Arby's and Wendy's, both experiencing malware-driven breaches of their POS systems. Based on the data breaches within the restaurant industry and Defendant's own history, Chipotle knew or should have known that it was at high risk for a similar malware data breach.

31. Chipotle previously suffered a data breach in 2004, which resulted in millions of dollars of losses to the company, and therefore should have been aware of the need to have adequate data security measures in place.[3]

32. In the 2004 data breach, hackers stole "Track 2" data from Chipotle's computer systems. Track 2 data includes the customer's name, card number, card expiration date, and card verification number. At the time, Chipotle explained that Internet gateways on its computers may not have been fully secure at all times. Additionally, Chipotle stated that it had "identified some store practices that may have made information systems at our stores vulnerable during periods before August 2004." An alarming revelation arising from the 2004 data breach was Chipotle's admission of the breadth of the breach, stating that it "began accepting credit cards in 1999, and it is possible that all of the cards we processed since then may have been vulnerable."[4]

33. Chipotle recently recognized the risk of a future data breach in its 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.

---

[3] Chipotle Mexican Grill, Inc., Annual Report (Form 10-K), p. 21 (Feb. 7, 2017), available at http://ir.chipotle.com/phoenix.zhtml?c=194775&p=irol-sec (last visited August 1, 2017).

[4] Chipotle Mexican Grill, Inc., Form S-1 Amendment 2, p. 15 (Dec. 23, 2005), available at: http://ir.chipotle.com/phoenix.zhtml?c=194775&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTM4NTU2MzAmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d (last visited August 1, 2017).

> 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.[5]

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

B. Stolen Customer Data Is Valuable to Hackers and Thieves

35. Chipotle is, and at all relevant times has been, aware that the PCD it maintains in its computer systems is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

36. It is well-known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by retailers, Chipotle maintained an insufficient and inadequate system to protect the PII of Plaintiffs and putative class members.

37. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's

[5] Chipotle Mexican Grill, Inc., Annual Report, *supra* fn. 3.

largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[6]

38. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, Chipotle's approach to maintaining the privacy of Plaintiffs' and putative class members' PII was lackadaisical, cavalier, reckless, and, at the very least, negligent.

C. Chipotle Failed to Comply with Industry Standards

39. In addition to ignoring breaches occurring at other retailers and its recognition of the vulnerabilities in its own systems which led to the 2004 data breach, Chipotle's security flaws also run afoul of industry best practices and standards. More specifically, the security practices at Chipotle are in stark contrast and direct conflict with the Payment Card Industry Data Security Standard.

40. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.[7]

41. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[8] PCI DSS sets the minimum level of what must be done, not the maximum.

---

[6] Verizon 2014 PCI Compliance Report, available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).
[7] *Payment Card Industry Data Security Standard* v3.2, p. 9 (May 2016) available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1492014699947 (last accessed April 10, 2017).
[8] *Id*.

42. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on Chipotle [9]:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	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

43. Furthermore, PCI DSS 3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates stated above. Chipotle was at all times fully aware of its data protection obligations for its restaurants in light of its participation in the payment card processing networks and its daily collection and transmission of PCD for at least 70% of its sales transactions.

44. Among other things, PCI DSS required Chipotle to properly secure and protect PCD; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt PCD at the point of sale.

45. PCI DSS also required Chipotle to not store "the full contents of … the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[10]

[9] *Id*.
[10] *Id*. at 38 (PCI DSS 3.2.1 and 3.2.2).

46. Further, Chipotle knew that because its stores accepted payment cards containing sensitive personal and financial information, customers, such as Plaintiffs and the other members of the putative class, were entitled to, and did, rely on Chipotle to keep that sensitive information secure from would-be thieves in accordance with all industry standards and requirements, such as the PCI DSS.

47. Despite Chipotle's awareness of its data security obligations, Chipotle's treatment of PCD and PII entrusted to it by its customers fell far short of satisfying Chipotle's legal duties and obligations, and included violations of the PCI DSS. Chipotle failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings, and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

D. Chipotle Failed to Upgrade Its Payment Systems to Use EMV Technology

48. The payment card industry also sets rules requiring all businesses to upgrade to new card readers that accept EMV chips. 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. EMV chip technology uses embedded computer chips instead of magnetic stripes to store PCD. The magnetic stripe on the back of a debit or credit card contains a code that is recovered by sliding the card through a magnetic stripe reader. The code never changes. Unlike magnetic stripe technology, in which the card information never changes, EMV technology creates a unique transaction code every time the chip is used. Such technology increases payment card security because the unique transaction code cannot be used again, making it more difficult for criminals to use stolen EMV chip card information.

49. 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.

50. In 2015, Chipotle reported that it would not upgrade its terminals to EMV technology, claiming that it would slow down customer lines.[11]

51. Under card operating regulations, businesses that continue accepting payment cards using magnetic stripe readers after the October 1, 2015 deadline are liable for damages resulting from any data breaches.

E. Chipotle Failed to Comply with FTC Requirements

52. In 2016, the Federal Trade Commission ("FTC") updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[12] The guidelines note 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 to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch

[11]Nicolas Upton, Busting Chip and Pin Upgrade Myths (September 2015), available at http://www.foodservicenews.net/The-FSN-Feed/September-2015/Busting-Chip-and-Pin-Upgrade-Myths/ (last visited June 1, 2017).

[12]Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 10, 2017).

for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC has supplemented those guidelines with its publication "Start With Security."[13] In these guidelines, the FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

54. 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.

55. 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 Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Chipotle's failure to follow the guidelines recommended by the FTC and failure to have reasonable data security measures in place constitute an unfair act or practice within the meaning of Section 5 of the FTC Act, 15 U.S.C. § 45.

F. The 2017 Chipotle Data Breach

57. While the investigation is still ongoing, Chipotle has announced that the Data Breach occurred as the result of malware placed on its POS systems.

58. 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

[13] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 10, 2017).

terminals since at least 2011, and specific types of malware have been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, and Michaels Stores. Additionally, the data breaches at Arby's and Wendy's resulted from the use of malware to infiltrate POS systems. As a result, Defendant was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

59. The Data Breach occurred because Chipotle failed to implement adequate data security measures to protect its POS network from the potential danger of a data breach, and failed to implement and maintain adequate systems to detect and prevent the breach and resulting harm that it has caused.

60. Had Chipotle implemented and maintained adequate safeguards to protect Customer Data, deter the hackers, and detect the data breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented.

61. In permitting the Data Breach to occur, Chipotle breached its implied agreement with customers to protect their personal and financial information and violated industry standards.

62. The Data Breach was caused and enabled by Chipotle's knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' Customer Data.

63. While many retailers have responded to recent breaches by adopting technology and security practices that help make transactions and stored data more secure, Chipotle has not done so.

64. Chipotle failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Customer Data compromised in the Data Breach.

G. The Chipotle Data Breach Caused Harm and Will Result in Additional Fraud

65. The ramifications of Chipotle's failure to keep Plaintiffs' and putative class members' data secure are severe.

66. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[15]

67. Personally identifiable information is a valuable commodity to identity thieves once the information has been compromised. The information Chipotle compromised, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the FTC. Identity theft occurs when someone uses another's PII, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

68. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

69. Identity thieves can use personal information, such as that of Plaintiffs and putative class members, which Chipotle failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a

[14] 17 C.F.R § 248.201 (2013).
[15] *Id.*
[16] FTC, Warning Signs of Identity Theft, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

70. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[17]

71. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[18]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

73. Plaintiffs and putative class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred

[17] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (April 10, 2017).
[18] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).
[19] GAO, Report to Congressional Requesters, at p.29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

H. Plaintiffs and Putative Class Members Suffered Damages

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

75. Plaintiffs' and putative class members' PII is private and sensitive in nature and was left inadequately protected by Chipotle. Chipotle did not obtain Plaintiffs' and putative class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

76. As a direct and proximate result of Chipotle's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and putative class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly

been recognized as compensable. For many consumers it is the way they are compensated, and, even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

77. Chipotle's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and putative class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and putative class members' information on the Internet card black market;

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

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. money paid for food purchased at Chipotle during the period of the Data Breach in that Plaintiffs and putative class members would not have dined at Chipotle, or at least would not have used their payment cards for purchases, had Chipotle disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Chipotle provided timely and accurate notice of the Data Breach;

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

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

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach; loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

78. Chipotle has not offered customers any credit monitoring or identity theft protection services, despite the fact that it is well-known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiffs and putative class members are left to their own actions to protect themselves from the financial damage Chipotle has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Chipotle's actions have created for Plaintiffs and putative class

members, is ascertainable and is a determination appropriate for the trier of fact. Chipotle has also not offered to cover any of the damages sustained by Plaintiffs or putative class members.

79. While the Customer Data of Plaintiffs and putative members of the Class has been stolen, Chipotle continues to hold Customer Data of consumers, including Plaintiffs and putative class members. Particularly because Chipotle has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and putative members of the Class have an undeniable interest in insuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CHOICE OF LAW

80. Chipotle's acts, misrepresentations, and omissions discussed herein were largely directed, approved, coordinated, and disseminated from its corporate headquarters in Colorado and the tortious and deceptive acts complained of occurred in, and radiated from, Colorado.

81. Chipotle's failure to employ adequate security measures, the key wrongdoing in these allegations, emanated from Chipotle's headquarters in Colorado.

82. Chipotle's principal executive offices, as well as its computer system, POS system, and IT personnel, operate out of, and are located at, Chipotle's headquarters in Colorado.

83. Application of Colorado law to a nationwide class, with respect to the claims brought herein, is appropriate, and neither arbitrary nor fundamentally unfair, because Colorado's interest in this litigation exceeds that of any other state.

CLASS ALLEGATIONS

84. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide Class defined as follows:

> All persons residing in the United States who made a credit or debit card purchase at any Chipotle or Pizzeria Locale affected location from March 24, 2017 through April 18, 2017 (the "Nationwide Class").

85. Excluded from the Class is Defendant and any of its parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned, as well as his or her judicial staff and immediate family members.

86. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

87. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

88. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of putative class members is unknown to Plaintiffs at this time, the proposed Class includes at least hundreds of thousands of customers whose data was compromised in the Chipotle Data Breach.

89. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Common questions of law and fact exist and predominate over any questions affecting only individual putative class members. The common questions include:

a. Whether Chipotle had a duty to protect Customer Data;

b. Whether Chipotle was negligent in failing to implement reasonable and adequate security procedures and practices;

c. Whether Chipotle knew or should have known that its computer systems were vulnerable to attack;

d. Whether Chipotle has an implied contractual obligation to use reasonable security measures;

e. Whether Chipotle has complied with any implied contractual obligation to use reasonable security measures;

f. Whether Chipotle conduct constituted deceptive trade practices under Colorado law;

g. Whether Chipotle's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Customer Data of Plaintiffs and putative class members;

h. Whether Chipotle's breaches of its legal duties caused Plaintiffs and the putative class members to suffer damages;

i. Whether Plaintiffs and putative class members are entitled to recover damages; and

j. Whether Plaintiffs and putative class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

90. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of those of other putative class members because Chipotle failed to safeguard Plaintiffs' information, like that of every other putative class member.

91. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation.

92. **Superiority. Fed. R. Civ. P. 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all

the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

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

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

95. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether putative class members' Customer Data was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendant knew about the Data Breach before it was announced to the public and failed to timely notify the public of the Breach;

c. Whether Defendant owed a legal duty to Plaintiffs and putative class members to exercise due care in collecting, storing, and safeguarding their Customer Data;

d. Whether Defendant breached a legal duty to Plaintiffs and putative class member to exercise due care in collecting, storing, and safeguarding their Customer Data;

e. Whether Defendant's conduct was an unlawful or unfair business practice under Colo. Rev. Stat. § 6-1-105(1)(l), *et seq*.;

f. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

g. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and putative class members' Customer Data secure and prevent the loss or misuse of that information;

h. Whether Defendant failed to take commercially reasonable steps to safeguard the Customer Data of Plaintiffs and the putative class members and thereby knowingly divulged the Customer Data of Plaintiffs and the putative class members while carried and maintained on Defendant's data systems;

i. Whether an implied contract existed between Defendant and Plaintiffs and putative class members and the terms of that implied contract; and,

j. Whether Defendant breached the implied contract.

96. Finally, all members of the proposed class are readily ascertainable. Chipotle has access to information regarding which of its restaurants were affected by the Data Breach, the time period of the breach, which customers were potentially affected, as well as the addresses and other contact information for members of the class, which can be used for providing notice to the putative class members.

COUNT I
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

97. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth herein.

98. Chipotle solicited and invited Plaintiffs and putative class members to eat at its restaurants and make purchases using their credit or debit cards. Plaintiffs and putative class members accepted Chipotle's offers and used their credit or debit cards to make purchases at Chipotle restaurants during the period of the Data Breach.

99. When Plaintiffs and putative class members paid for purchases of Chipotle's services and products in connection with their meals at Chipotle properties, they provided their Customer Data, including, but not limited to, the PII and PCD contained on the face of, and embedded in the magnetic stripe of, their debit and credit cards. In so doing, Plaintiffs and putative class members entered into implied contracts with Chipotle pursuant to which Chipotle agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and putative class members if their data had been breached and compromised.

100. Each purchase at Chipotle restaurants made by Plaintiffs and putative class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Chipotle under which Chipotle agreed to safeguard and protect the Customer Data of Plaintiffs and putative class members, including all information contained in the magnetic stripe of Plaintiffs' and putative class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

101. Plaintiffs and putative class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards, to Chipotle to eat at its restaurants and make purchases in the absence of the implied contract between them and Chipotle.

102. Plaintiffs and putative class members fully performed their obligations under the implied contracts with Chipotle.

103. Chipotle breached the implied contracts it made with Plaintiffs and putative class members by failing to safeguard and protect the PII and PCD of Plaintiffs and putative class members and by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

104. As a direct and proximate result of Chipotle's breaches of the implied contracts between Chipotle and Plaintiffs and putative class members, Plaintiffs and putative class members sustained actual losses and damages as described in detail above.

COUNT II
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

105. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth herein.

106. Upon accepting and storing the Customer Data of Plaintiffs and putative class members in its computer systems, Chipotle undertook and owed a duty to Plaintiffs and putative class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Chipotle knew that the Customer Data was private and confidential and should be protected as private and confidential.

107. The law imposes an affirmative duty on Chipotle to timely disclose the unauthorized access and theft of the Customer Data to Plaintiffs and the Class so that Plaintiffs and putative class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Customer Data.

108. Chipotle has a common law duty to prevent the foreseeable risk of harm to others, including the Plaintiffs and putative class members. It was certainly foreseeable to Chipotle that injury would result from a failure to use reasonable measures to protect Customer Data. It was also

reasonably foreseeable that, if reasonable security measures were not taken, hackers would steal PCD belonging to Chipotle customers.

109. Chipotle assumed the duty to use reasonable security measures as a result of its conduct and decision to accept payment cards for purchases.

110. Chipotle also had duty to use reasonable data security measures arising 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 PCD by businesses such as Chipotle. The FTC publications and data security breach orders described above further form the basis of Chipotle's duty.

111. Chipotle breached its duty to Plaintiffs and the putative class members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Customer Data. Furthering its dilatory practices, Chipotle failed to provide adequate supervision and oversight of the Customer Data with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Customer Data of Plaintiffs and putative class members, misuse the Customer Data and intentionally disclose it to others without consent.

112. Chipotle breached its duties to Plaintiffs and putative class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Plaintiffs and putative class members.

113. Through Chipotle's acts and omissions described in this Complaint, including Chipotle's failure to provide adequate security and its failure to protect Customer Data of Plaintiffs and putative class members from being foreseeably captured, accessed, disseminated, stolen and

misused, Chipotle breached its duty to use reasonable care to adequately protect and secure Customer Data of Plaintiffs and putative class members during the time it was within Chipotle's possession or control.

114. Chipotle 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.

115. Upon information and belief, Chipotle improperly and inadequately safeguarded Customer Data of Plaintiffs and putative class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Chipotle's failure to take proper security measures to protect sensitive Customer Data of Plaintiffs and putative class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Customer Data of Plaintiffs and putative class members.

116. Chipotle failed to take proper security measures to protect Customer Data of Plaintiffs and putative class members.

117. Chipotle's conduct was grossly negligent and departed from all reasonable standards of care including, but not limited to: failing to adequately protect the Customer Data; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Customer Data of Plaintiffs and putative class members; and failing to provide Plaintiffs and putative class members with timely and sufficient notice that their sensitive Customer Data had been compromised.

118. Neither Plaintiffs nor the other putative class members contributed to the Data Breach and subsequent misuse of their Customer Data as described in this Complaint.

119. As a direct and proximate cause of Chipotle's conduct, Plaintiffs and putative class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiffs and putative class members; damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach including but not limited to, late fees charged and foregone cash-back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
Violation of Colorado Consumer Protection Act,
Colo. Rev. Stat. § 6-1-105(1)(l), *et seq*.
(On behalf of Plaintiffs and the Nationwide Class)

120. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth here.

121. Plaintiffs and putative class members are consumers who used their credit or debit cards to purchase food and drink products for personal, family, and household purposes from Chipotle locations.

122. Chipotle engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food products, goods, or services to consumers, including Plaintiffs and putative class members.

123. Chipotle is engaged in, and its acts and omissions affect, trade and commerce. Chipotle's relevant acts, practices, and omissions complained of in this action were done in the course of Chipotle's business of marketing, offering for sale, and selling food products, goods, and services throughout the United States.

124. The Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-105(1)(l), *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service.

125. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers, Chipotle's actions were directed at consumers.

126. In the conduct of its business, trade, and commerce, and in the sale of food products, goods, or services to consumers, Chipotle collected and stored highly personal and private information, including Customer Data belonging to Plaintiffs and putative class members.

127. Chipotle knew or should have known that its computer systems and data security practices were inadequate to safeguard the Customer Data of its customers and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

128. Chipotle should have disclosed this information regarding its computer systems and data security practices because Chipotle was in a superior position to know the true facts related to the defect, and Plaintiffs and putative class members could not reasonably be expected to learn or discover the true facts.

129. As alleged in this Complaint, Chipotle engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, goods, or services to consumers in violation of the Colorado Consumer Protection Act including, but not limited to, the following:

a. failing to adequately secure the Customer Data;

b. failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

c. failing to disclose the material information, known at the time of the consumer transaction, that its computer systems would not adequately protect and safeguard Customer Data;

d. inducing consumers to make purchases and enter into payment card transactions by failing to disclose, and misrepresenting the material fact, that Chipotle's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft; and,

e. continuing to accept credit and debit card payments and storage of other personal information after Chipotle knew or should have known of the data breach and before it allegedly remedied the breach.

130. By engaging in the conduct delineated above, Chipotle has violated the Colorado Consumer Protection Act by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the financial transactions, particularly the security thereof, between Chipotle and its customers for the purchase of food products, goods, and services;

c. misrepresenting material facts in the furnishing or sale of food products, goods, or services to consumers;

d. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. engaging in conduct with the intent to induce consumers to make transactions using payment cards;

g. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

h. other unfair, deceptive, unconscionable, fraudulent, and/or unlawful acts or practices to be shown at trial. Chipotle systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiffs and putative class members.

131. Chipotle's actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and putative class members.

132. As a direct result of Chipotle's violation of the Colorado Consumer Protection Act, Plaintiffs and putative class members have suffered actual damages that include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information by criminals;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with unauthorized use of their financial accounts;

e. costs associated with the cancellation and reissuing of payment cards;

f. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

g. lost value of benefits from use of payment cards;

h. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing, and seeking reimbursement for fraudulent charges, canceling, and activating payment cards, and shopping for credit monitoring and identity theft protection;

i. the certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and being already misused;

j. impairment to their credit scores and ability to borrow and/or obtain credit; and,

k. the continued risk to their personal information, which remains on Chipotle's insufficiently secured computer systems.

133. As a result of Chipotle's violations of the Colorado Consumer Protection Act, Plaintiffs and putative class members are entitled to, and seek, injunctive relief including, but not limited to:

a. Ordering that Chipotle engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Chipotle systems on a periodic

basis, and ordering Chipotle to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Chipotle engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Chipotle audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Chipotle segment customer data by, among other things, creating firewalls and access controls so that if one area of Chipotle is compromised, hackers cannot gain access to other portions of Chipotle's systems;

e. Ordering that Chipotle purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of services;

f. Ordering that Chipotle conduct regular database scanning and securing checks;

g. Ordering that Chipotle routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Chipotle to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

134. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Chipotle alleged herein, Plaintiffs and putative class members seek relief under Colo. Rev. Stat. § 6-1-113, including, but not limited to, the greater of actual damages, statutory damages, or treble damages for bad faith conduct, injunctive relief, and attorneys' fees and costs, as allowable by law.

COUNT V
Declaratory Judgment
(On behalf of Plaintiffs and the Nationwide Class)

135. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth here.

136. As previously alleged, Plaintiffs and putative class members entered into an implied contract that required Chipotle to provide adequate security for the Customer Data it collected from their payment card transactions. As previously alleged, Chipotle owes duties of care to Plaintiffs and putative class members that require it to adequately secure Customer Data.

137. Chipotle still possesses Customer Data pertaining to Plaintiffs and putative class members.

138. Chipotle has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its POS systems.

139. Accordingly, Chipotle has not satisfied its contractual obligations and legal duties to Plaintiffs and putative class members. In fact, now that Chipotle's lax approach towards data security has become public, the Customer Data in its possession is more vulnerable than previously.

140. Actual harm and controversy has arisen in the wake of the Data Breach regarding Chipotle's common law and other duties to reasonably safeguard the Customer Data of Plaintiffs and putative class members.

141. 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, this Court has broad authority to restrain acts which are tortious and which violate the terms of federal and state statutes described herein.

142. Plaintiffs, therefore, seek a declaration from this Court that, among other things:

a. Chipotle continues to owe a legal duty to secure its customers' Customer Data;

b. Chipotle's existing data security measures do not comply with this legal duty; and,

c. Chipotle's ongoing breach of this legal duty continues to harm Plaintiffs and putative class members.

143. Plaintiffs also request the Court to issue corresponding injunctive relief requiring Chipotle to, among other things:

a. implement encryption for the transmission of cardholder data in accordance with industry standards;

b. engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Chipotle's systems on a periodic basis;

c. promptly correct any problems or issues detected by such third-party security auditors;

d. engage third-party security auditors and internal personnel to run automated security monitoring;

e. audit, test, and train its security personnel regarding any new or modified procedures;

f. segment Customer Data by, among other things, creating firewalls and access controls so that if one area of Chipotle is compromised, hackers cannot gain access to other portions of Chipotle's systems;

g. purge, delete, and destroy in a reasonable secure manner Customer Data not necessary for its provisions of services;

h. routinely and continually conduct training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

i. educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Chipotle's customers must take to protect themselves in wake of the Data Breach.

144. The Customer Data of Plaintiffs and putative class members continues to be contained on Chipotle's data systems. If an injunction is not issued, Plaintiffs and putative class members will suffer irreparable harm. The risk of another such breach is real, immediate, and substantial, as evidenced by Chipotle having sustained a prior breach of its data systems in 2004. Plaintiffs and putative class members lack an adequate legal remedy in the event of another data breach at Chipotle because many of the resulting injuries are not readily quantifiable. Monetary damages, while warranted to compensate Plaintiffs and putative class members for out-of-pocket damages, do not cover the full extent of their injuries.

145. The hardship to Plaintiffs and putative class members, if an injunction is not issued, exceeds the hardship to Chipotle, if an injunction is issued. An injunction would benefit the public by preventing another data breach at Chipotle, thus eliminating the injuries that would result to consumers whose confidential information would be compromised. On the other hand, the cost of Chipotle to comply with an injunction, by employing reasonable data security measures, which already has a pre-existing legal obligation to employ, is minimal.

COUNT VI
Negligence Per Se
(On behalf of Plaintiffs and the Nationwide Class)

146. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth herein.

147. 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 Customer Data. The FTC publications and orders described above also form part of the basis of Chipotle's duty in this regard.

148. Chipotle violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. Chipotle's conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, and the foreseeable consequences of a data breach at a restaurant chain as large as Chipotle, including, specifically, the immense damages that would result to Plaintiffs and putative class members.

149. Chipotle's violation of Section 5 of the FTC Act constitutes negligence *per se*.

150. Plaintiffs and putative class members are within the class of persons that the FTC Act was intended to protect.

151. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued 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 Plaintiffs and putative class members.

152. As a direct and proximate result of Chipotle's negligence *per se*, Plaintiffs and putative class members have suffered, and continue to suffer, injuries and damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach including, but not limited to, late fees charged and foregone cash-back rewards; damages from lost time and effort to mitigate the actual and potential impact of the

Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT VII
Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Class)

153. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth here.

154. Plaintiffs and putative class members conferred a monetary benefit on Chipotle. Specifically, they purchased goods and services from Chipotle and provided Chipotle with their payment information. In exchange, Plaintiffs and putative class members should have received from Chipotle the goods and services that were the subject of the transaction and should have been entitled to have Chipotle protect their Customer Data with adequate data security.

155. Chipotle knew that Plaintiffs and putative class members conferred a benefit on Chipotle. Chipotle profited from the purchases and used the Customer Data of Plaintiffs and putative class members for business purposes.

156. Chipotle failed to secure the Customer Data of Plaintiffs and putative class members and, therefore, did not provide full compensation for the benefit the Plaintiffs and putative class members provided.

157. In addition to the monetary benefit of the purchases made by Plaintiffs and putative class members, Chipotle received the benefit of not incurring the cost of adequate and proper data security measures at the expense of Plaintiffs and putative class members.

158. Chipotle acquired the Customer Data through inequitable means as it failed to disclose the inadequate security practices previously alleged.

159. If Plaintiffs and putative class members had known that Chipotle would not secure their Customer Data using adequate security, they would not have made purchases at Chipotle-owned restaurants.

160. Plaintiffs and putative class members have no adequate remedy at law.

161. Under the circumstances, it would be unjust for Chipotle to be permitted to retain any of the benefits that Plaintiffs and putative class members conferred on it and that Chipotle received at the expense of Plaintiffs and putative class members.

162. Chipotle should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and putative class members, proceeds that it unjustly received from them. In the alternative, Chipotle should be compelled to refund the amounts that Plaintiffs and putative class members overpaid.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all putative class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Chipotle as follows:

a. For an Order certifying the Nationwide Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class;

b. For equitable relief enjoining Chipotle from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and putative class members' Customer Data, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and putative class members;

c. For equitable relief compelling Chipotle to use appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity to putative class members the type of PII and PCD compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of costs of suit and attorneys' fees, as allowable by law; and, such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demands a jury trial on all issues so triable.

This the 18th day of August, 2017.

/s Kevin S. Hannon
Kevin S. Hannon
Colorado Bar No. 16015
THE HANNON LAW FIRM, LLC
1641 Downing Street
Denver, CO 80218
Tel: 303-861-8800
khannon@hannonlaw.com

John Yanchunis
Marisa Glassman*
Florida Bar No. 111991
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@forthepeople.com
mglassman@forthepeople.com

Ben Barnow*
Illinois Bar No. 0118265
Erich P. Schork*
Illinois Bar No. 6291153
Anthony L. Parkhill*
Illinois Bar No. 6317680
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000

b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com

Jean Sutton Martin*
North Carolina Bar Number 25703
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road, Suite 225
Wilmington, NC 28403
Tel: (910) 292-6676
jean@jsmlawoffice.com

Christopher D. Jennings*
Arkansas Bar Number 2006306
JOHNSON VINES PLLC
2226 Cottondale Lane, Suite 210
Little Rock, AR 72202
Tel: (501) 372-1300
cjennings@johnsonvines.com

Paul C. Whalen *
LAW OFFICE OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, NY 11030
Tel: (516) 426-6870
paul@paulwhalen.com

Jasper D. Ward IV*
JONES WARD PLC
312 S. Fourth Street
Louisville, KY 40202
Tel: (502) 882-6000
jasper@jonesward.com

Brian P. Murray*
GLANCY PRONGAY & MURRAY LLP
122 East 42nd Street, Suite 2920
New York, NY 10168
Tel: (212) 682-5340
bmurray@glancylaw.com

** bar admission to be submitted*

Attorneys for Plaintiffs and the Proposed Class

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Greg Lawson and Judy Conard, individually and on behalf of all others similarly situated

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Kevin S. Hannon The Hannon Law Firm, LLC
1641 Downing Street
Denver, CO 80218

DEFENDANTS

Chipotle Mexican Grill, Inc.

County of Residence of First Listed Defendant Arapahoe County, CO
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*
Paul Karlsgodt Baker & Hostetler
1801 California Street, Suite 400
Denver, CO 80202

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

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

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
☒ 190 Other Contract	❒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise				❒ 864 SSID Title XVI	❒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
					❒ 893 Environmental Matters
					❒ 895 Freedom of Information Act
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 896 Arbitration
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 950 Constitutionality of State Statutes
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 USC Section 1332(d)(2)

Brief description of cause:
Data Breach - negligence, breach of implied contract, dec judgment, violation Colo Consumer Protection Act

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ Greater than $5M

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Christine M. Arguello; William J. Martinez DOCKET NUMBER 1:17-cv-1415; 1:17-cv-1102

DATE 08/18/2017

SIGNATURE OF ATTORNEY OF RECORD Kevin S. Hannon

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

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

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

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

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

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

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

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

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

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

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

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Colorado

Greg Lawson and Judy Conard, individually and on behalf of all others similarly situated

Plaintiff(s)

v.

Chipotle Mexican Grill, Inc.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Chipotle Mexican Grill, Inc.
c/o Registered Agent Bryant Messner
1430 Wynkoop St.
Suite 400
Denver, Colorado 80202

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Kevin S. Hannon
The Hannon Law Firm, LLC
1641 Downing Street
Denver, Colorado 80218
303-861-8800

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: