IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 1:17-cv-01415-CMA-MLC

TODD GORDON, MARC and KRISTEN MERCER, h/w, KRISTIN BAKER, MICHELLE FOWLER, GREG LAWSON and JUDY CONARD, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CHIPOTLE MEXICAN GRILL, INC.,

Defendant.

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

Plaintiffs Todd Gordon, Marc and Kristen Mercer, Kristin Baker, Michelle Fowler, Greg Lawson, and Judy Conard ("Plaintiffs"), individually and on behalf of all others similarly situated, based on personal knowledge as to their own experiences and on investigation of counsel as to all other matters, allege the following against Defendant Chipotle Mexican Grill, Inc. ("Chipotle" or "Defendant"):

NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose personal and non-public information, including credit card and debit card numbers, credit card and debit card expiration dates, credit and debit card security information, and other credit and debit card information (collectively, "Card Information")

was compromised in a massive security breach of Defendant's computer servers beginning on or around March 24, 2017 and lasting until April 18, 2017 (the "Chipotle Data Breach" or "Data Breach").

2. As alleged herein, the injuries to Plaintiffs and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for customer information, including Card Information; to secure and safeguard customers' Card Information and other personal information; and to timely and accurately notify Plaintiffs and Class Members that their personal and financial information had been compromised.

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

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

customer Card Information to be stolen.

5. Defendant exposed customers to greater damages by, upon information and belief, failing to implement chip-based card technology, otherwise known as "EMV" technology. EMV – which stands for Europay, MasterCard, and Visa – is a "global standard" for cards equipped with computer chips and technology used to authenticate chip card transactions.[1] Despite this technology's growing prominence and availability, upon information and belief, Defendant has not implemented EMV technology in its stores, leaving all of the information collected or transmitted via payment card magnetic stripes from payment cards used in its restaurant locations vulnerable to theft. In 2015, Chipotle reported that it would not upgrade its terminals to EMV technology, claiming that it would slow down customer lines.[2]

6. As a direct and proximate consequence of Defendant's negligence, a massive amount of customer information was stolen from Chipotle. An investigation is still ongoing, but upon information and belief, the Chipotle Data Breach may have compromised the Card Information of thousands of Chipotle customers, if not more. Indeed, Chipotle spokesperson Chris Arnold has acknowledged that "most" of its 2,249 restaurants, including both the Chipotle and Pizzeria Locale brands, were affected by the breach in the 48 contiguous states.[3] Victims of this data breach have had their Card

[1] http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php (last visited Oct. 24, 2017).
[2] http://www.foodservicenews.net/The-FSN-Feed/September-2015/Busting-Chip-and-Pin-Upgrade-Myths/ (last visited on Oct. 24, 2017).
[3] http://www.nrn.com/operations/chipotle-data-breach-affected-locations-nationwide (last visited Oct. 22, 2017); https://www.eater.com/2017/4/26/15433866/chipotle-data-

Information compromised, have had their privacy rights violated, have been exposed to the increased risk of fraud and identify theft (with many consumers actually having suffered incidents of fraud or identity theft), and have otherwise suffered damages.

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

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

9. Plaintiffs and the members of the Class seek to recover damages resulting from Defendant's negligence, negligence *per se*, breach of contract, violation of state laws, and for declaratory and injunctive relief.

PARTIES

Plaintiffs

10. Plaintiff Todd Gordon is an adult residing in Laveen, Arizona. On or about March 26, 2017, Plaintiff Gordon used his American Express credit card at Chipotle's

---

breach-credit-cards (last visited Oct. 24, 2017); https://www.thedailymeal.com/news/eat/if-you-have-been-chipotle-past-few-months-you-may-be-victim-identify-theft/053017 (last visited Oct. 24, 2017).

Laveen, Arizona restaurant location. Per the Chipotle website, this location was affected by the Chipotle Data Breach during that time period. Less than two months later, Plaintiff Gordon's same American Express credit card was fraudulently used in Miami, Florida, causing Plaintiff Gordon's credit card account to exceed the account limit. On or about May 13, 2017, fraudsters charged $507.72 of purchases at a Nike factory store and $339.72 of purchases at Toys "R" Us to Plaintiff's credit card. As a result of Plaintiff Gordon's credit card account exceeding its limit through no fault of Plaintiff Gordon's own, American Express made a report to the credit bureaus, thereby negatively affecting Plaintiff Gordon's credit score and information.

11. Prior to the fraudulent transactions, Plaintiff Gordon had not experienced credit card fraud or identity theft with respect to his American Express credit card account. In fact, Plaintiff Gordon had been recently issued a brand new credit card and credit card number under his American Express account approximately six months prior to the fraudulent transactions. Furthermore, Plaintiff Gordon has no prior history of being victimized by credit card fraud. As a result of having been victimized by the Chipotle Data Breach, Plaintiff Gordon was required to spend a significant amount of time – approximately five to six hours – addressing the unauthorized transactions. Plaintiff Gordon has yet to be reimbursed for the fraudulent transactions and as a result of the Data Breach, his credit score was lowered and he was forced to take a higher finance rate on a car loan. Had Plaintiff Gordon known that Chipotle does not adequately protect Card Information and other sensitive information, he would have never made a purchase at Chipotle using his credit card. As a result of Chipotle's failure to adequately safeguard

Plaintiff Gordon's Card Information, Plaintiff Gordon has been injured. To date, Plaintiff Gordon has not received any notice from Defendant about the Data Breach.

12. Plaintiffs Marc and Kristen Mercer ("Mercer Plaintiffs") are individuals and residents of San Jose, California. Mercer Plaintiffs used their debit card at Chipotle locations at 1050 Park Place, San Mateo, California, and 975 The Alameda Suite 10, San Jose, California on April 1, 5, 7, and 13, 2017. On June 15, 2017, the Mercer Plaintiffs received a letter from their bank stating that, due to Chipotle Data Breach, their card data may have been exposed. Plaintiffs were informed that their debit card would need to be deactivated, and a new debit card would be sent. On or about June 24, 2017, Plaintiff Marc Mercer received a call from his bank regarding suspicious activity on his account, and he learned that someone had attempted to charge a $200 purchase at Wal-Mart. After learning this, Plaintiff Marc Mercer logged onto his bank account and found that numerous other fraudulent charges had been made and approved, and that there were additional fraudulent charges pending. The Mercer Plaintiffs contacted the bank to have their card deactivated immediately. After deactivating their card, Plaintiffs had no access to their debit card funds until a new bank card arrived.

13. On June 26, 2017, Plaintiff Marc Mercer went to his bank and reviewed pending and posted fraudulent charges with a bank representative. After going through the charges and identifying all of the inaccurate charges, a new card was issued. However, as a result of the Chipotle Data Breach and the fraud on Plaintiffs' account, many of their normal services had been disrupted, automated orders (*e.g.,* prescription animal food for one of their pets) were delayed and cancelled due to nonpayment,

among other things. The Mercer Plaintiffs were ultimately able to get the fraudulent charges reimbursed but it took a number of weeks and roughly six hours of Plaintiffs' personal time to obtain the reversal. Had the Mercer Plaintiffs known that Chipotle does not adequately protect Card Information and other sensitive information, they would have never made a purchase at Chipotle using their debit card. As a result of Chipotle's failure to adequately safeguard the Mercer Plaintiffs' Card Information, the Mercer Plaintiffs have been injured.

14. Plaintiff Kristin Baker is an individual and resident of Riverside County, California. On or about March 29, 2017, Plaintiff Baker used her debit card to make a food purchase at the Chipotle restaurant located at 8956 Trautwein Road, Riverside, California. Only a few days later, fraudulent activity appeared on the same debit card account. On April 3, 2017, three unauthorized charges were attempted on Plaintiff's debit card. She learned about the attempts via email alerts from her bank, for online purchases of $69.99, $19.99, and $49.99, respectively. The charge of $49.99 went through, but the others were declined. Ultimately, Plaintiff's bank refunded the unauthorized charge. To date, Plaintiff Baker has not received any notice from Defendant about the Data Breach. Had Plaintiff Baker known that Chipotle does not adequately protect Card Information and other sensitive information, she would have never made a purchase at Chipotle using their debit card. As a result of Chipotle's failure to adequately safeguard Plaintiff Baker's Card Information, Plaintiff Baker has been injured.

15. Plaintiff Michelle Fowler is an individual and resident of Chicago, Illinois. On

April 3, 12, and 18, 2017, Plaintiff Fowler used her MasterCard to make a food purchase at the 2153 311 South Wacker Drive Chipotle location in Chicago. On May 8, Plaintiff reviewed her online statement and noticed that on or about May 6, 2017, someone had made $517.86 of fraudulent charges to her account. She cancelled her card and initiated a dispute of all fraudulent charges with the credit card company. When Plaintiff called her credit card company to ask for details relating to the fraud, she was told that they could not provide details, and was provided a refund of only $8. Plaintiff Fowler called the credit card company again the next day and spent over an hour talking to four different representatives, none of whom were aware of the credit card data breach. The following day, on May 10, Plaintiff spent another half hour talking with a bank representative in the fraud department. Plaintiff was subsequently refunded the losses she sustained due to the fraud. Then, on July 22, 2017, multiple credit cards were fraudulently opened in Plaintiff's name at 6 different stores (Best Buy, Lowes, Target, Home Depot, Walmart, and Kohl's). Plaintiff continues to deal with the fallout from these attempted and successful fraudulent account openings, as it takes weeks for companies to resolve the fraud claims and remove the erroneous inquiries and accounts from her credit report.

16. As a result of having been victimized by the Chipotle Data Breach, Plaintiff Fowler was required to spend a significant amount of time – at least 30 hours total – making phone calls, monitoring her card transactions, and addressing the unauthorized transactions and account openings/related activity. Plaintiff was also forced to switch over all of her recurring charges from her cancelled card and missed a couple of payments due to this issue. Furthermore, Plaintiff has had to place security freezes with all 3 credit

bureaus at her own cost, which will result in difficulty for her opening legitimate accounts under her name when she desires to do so. As a result of Chipotle's failure to adequately safeguard Plaintiff Fowler's Card Information, Plaintiff Fowler has been injured. To date, Plaintiff Fowler has not received any notice from Defendant about the Data Breach.

17. 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 Plaintiff Lawson uses for daily expenditures because of the cash back rewards benefit. Within a few weeks of this visit, Plaintiff 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 Plaintiff Lawson that it would be closing the account, opening a new account, and re-issuing a new debit card. Because Plaintiff 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. Therefore, Plaintiff Lawson did not have his debit card to use for his travel expenses as he planned. As a result of having been victimized by the Chipotle Data Breach, Plaintiff Lawson has been required to spend time communicating with his bank regarding his compromised card, account transfer, and replacement card. Had Plaintiff Lawson known that Chipotle does not adequately protect Card Information and other sensitive information, he would have never made a purchase at Chipotle using his credit card. As a result of Chipotle's failure to adequately safeguard Plaintiff Lawson's Card Information, Plaintiff Lawson has been

injured. To date, Plaintiff Lawson has not received any notice from Defendant about the Data Breach.

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 Plaintiff Conard uses for daily expenditures because of the rewards benefit. On or about April 22, 2017, Plaintiff Conard received a call from her bank seeking approval for a $1,300 charge from Barcelona, Spain. Determining that Plaintiff Conard's credit card had been compromised, her bank closed the card account and re-issued a new credit card. Plaintiff Conard was required to spend time communicating with her bank regarding her compromised card and replacement card. She has spent time contacting businesses to notify them and provide the information for her new card for established automatic payments linked to her credit card. She has spent roughy 20 hours remedying the effects of her credit card being compromised as a result of the Chipotle Data Breach. While awaiting a replacement card, Plaintiff 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, Plaintiff Conard has contracted for identity theft monitoring services through LifeLock at an annual cost of $131.93. Had Plaintiff Conard known that Chipotle does not adequately protect Card Information and other sensitive information, she would have never made a purchase at Chipotle using her credit card. As a result of Chipotle's failure

to adequately safeguard Plaintiff Conard's Card Information, Plaintiff Conard has been injured. To date, Plaintiff Conard has not received any notice from Defendant about the Data Breach.

Defendant

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

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which there are more than 100 putative class members, many of which are citizens of a different state than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Defendant because Chipotle maintains its principal place of business in Colorado. Defendant has sufficient minimum contacts with the state of Colorado and intentionally avails itself of the consumers and

markets within the state through the promotion, marketing, and sale of its food services.

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

FACTUAL ALLEGATIONS

A. The Data Breach and Chipotle's Disclosures

23. Defendant's 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.

24. When Chipotle's 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.

25. Beginning on or about March 24, 2017, hackers utilizing malicious software accessed the point-of-sale ("POS") systems at Chipotle and Pizzeria Locale locations throughout the United States and stole copies of customers' Card Information and other personal information. The software used in the attack was a malware strain designed to siphon data from cards when they are swiped at infected POS systems. According to Defendant, the hackers maintained operation of the malware in Defendant's POS devices at a majority, if not all, of Chipotle and Pizzeria Locale locations through April 18, 2017.

26. Based upon information and belief, hackers had previously utilized similar malware in other recent cyber-attacks, including the retail data breaches at Target and Home Depot. While many retailers, banks, and card companies have responded to these recent breaches by adopting technology and security practices that help makes transactions and stored data more secure, Defendant did not do so.

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

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

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

> We want to make our customers aware that we recently detected unauthorized activity on the network that supports payment processing for purchases made in our restaurants. We immediately began an investigation with the help of leading cyber security firms, law enforcement, and our payment processor. We believe actions we have taken have stopped the unauthorized activity, and we have implemented additional security enhancements. Our investigation is focused on card transactions in our restaurants that occurred

> from March 24, 2017 through April 18, 2017. . . . We anticipate providing notification to any affected customers as we get further clarity about the specific timeframes and restaurant locations that may have been affected. Consistent with good practices, consumers should closely monitor their payment card statements. If anyone sees an unauthorized charge, they should immediately notify the bank that issued the card. Payment card network rules generally state that cardholders are not responsible for such charges.

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

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

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

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

34. If fraud was occurring and on-going from late March to mid-April of 2017, it is likely that, at least, credit card company analytics and other methods (undercover investigations of the black market) would have discovered the Breach before April 25,

2017. Defendant has failed to provide a cogent picture of how the Data Breach occurred, when it was discovered, and its full effects on customers' personal and financial information.

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

36. Thieves already are using the information stolen from Defendant to commit actual fraud. For example, a story was recently reported by SC Media about a fraudster who used payment card account login credentials of more than 40 people that were stolen during the Chipotle Breach – and believed to have been purchased from the Dark Web – to steal $17,000 from an ATM in Gainesville, Florida.[4]

B. Chipotle's Collection of Customer Card Information

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

[4] https://www.scmagazine.com/chipotle-data-breach-leads-to-illegal-atm-withdrawal/article/676626/ (last visited Oct. 24, 2017).

to finish the transaction on behalf of the customer.

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

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

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

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

40. Thus, Defendant stores massive amounts of Card Information and other personal information on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

41. Consumers place value in data privacy and security, and they consider it

when making purchasing decisions. Plaintiffs would not have made their purchases at Defendant's restaurant, or would not have paid as much, had they known that Defendant does not take all necessary precautions to secure their personal and financial data. Defendant failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Defendant's restaurants.

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

C. The Known Value of Card Information

43. It is well known that customer Card Information is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including Arby's, Wendy's, Target, Neiman Marcus, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, Kmart, and many others.

44. Legitimate organizations and the criminal underground alike recognize the value in customer Card Information and other personal information. Otherwise, they

wouldn't pay for it or aggressively seek it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[5] Similarly, in the Target data breach, in addition to Card Information data pertaining to 40,000 credit and debit cards, hackers stole personal information pertaining to 70,000 customers.

45. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[6]

46. As with the ATM theft in Florida (*see* ¶ 36, *supra*), fraudsters will turn to the Dark Web or other criminal resources to purchase stolen financial and personal information to perpetrate financial frauds.[7]

47. 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.

48. Indeed, 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.[8]

---

[5] 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 Oct. 24, 2017).
[6] *Id.*
[7] *See, e.g.,* "Inside The Dark Net Markets For Stolen Credit Cards", available at http://www.vocativ.com/311187/dark-net-credit-card/ (last visited Oct. 24, 2017) (discussing the sale of hacked credit card data on online criminal black markets).
[8] 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 Oct. 24, 2017).

49. Chipotle also 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.
>
> 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.[9]

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

51. At all relevant times, Chipotle was well-aware, or reasonably should have

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

been aware, that the Card Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

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

D. Chipotle's Deficient Security Protocols and Failure to Adequately Secure and Safeguard Customer Information

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

54. Defendant's security protocols were so deficient that the Data Breach continued for over three weeks while Defendant failed to even detect it—this despite widespread knowledge of the malicious software (or malware) used to perpetrate the Data Breach, which, upon information and belief, was similar to the malware used to perpetrate the earlier, notorious, and widely reported data breaches affecting retailers Target and Home Depot.

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

56. Defendant could have prevented this Data Breach. Based upon information and belief, the malicious software used in the Data Breach was similar to the malware strains hackers used in the data breaches at Target and Home Depot. While many

retailers, banks, and card companies responded to recent breaches, including the Target and Home Depot breaches, by adopting technology that helps makes transactions more secure, Defendant did not.

57. Defendant disregarded Plaintiffs' and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Card Information. On information and belief, Plaintiffs' and Class members' Card Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class members' Card Information was compromised and stolen.

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

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

regularly monitor and test networks, and ensure the maintenance of information security policies.

60. 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."[10] PCI DSS sets the minimum level of what must be done, not the maximum.

61. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on Chipotle [11]:

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

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

[10] *Id.*
[11] *Id.*

transmission of tens of thousands of sets of Card Information.

63. Among other things, PCI DSS required Chipotle to properly secure and protect Card Information; 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 Card Information at the point of sale.

64. 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.[12]

65. 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.

66. Despite Chipotle's awareness of its data security obligations, Chipotle's treatment of Card Information 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 were reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems

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

to detect and deter the type of attack that occurred and is at issue here.

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

68. EMV chip technology uses embedded computer chips instead of magnetic stripes to store Card Information. Unlike magnetic stripe cards that use static data (*i.e.*, the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen.

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

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

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

72. In 2007, the FTC published guidelines that establish reasonable data

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

73. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[13]

74. 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.

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

[13] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Nov. 2011), www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personalinformation-guide-business_0.pdf (last visited Oct. 24, 2017).

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

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

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

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

80. While the investigation is still ongoing, Chipotle has announced that the Data Breach occurred as the result of malware placed on its POS systems. As cards were swiped through card readers, the malware searched for tracked data, including cardholder names, numbers, expirations dates, and card verification codes from the cards' magnetic strips.[14]

81. Defendant was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used to access POS terminals since at least 2011, and specific types of malware, including RAM scraper malware, have been used recently to infiltrate large retailers such as Target, Sally

[14] http://fox59.com/2017/06/01/more-than-30-indiana-locations-affected-by-chipotle-data-breach/ (last visited Oct. 24, 2017).

Beauty, Neiman Marcus, Michaels Stores, and Supervalu. 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.

82. In addition to the publicly announced data breaches described above, Defendant received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[15]

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

84. Defendant, at all times relevant to this action, had a duty to Plaintiffs and members of the Class to: (a) properly secure payment card magnetic stripe information at the point of sale and on Defendant's internal networks; (b) encrypt Card Information using industry standard methods; (c) properly use and deploy up-to-date EMV technology; (d) use available technology to defend its POS terminals from well-known

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

methods of invasion; and (e) act reasonably to prevent the foreseeable harms to Plaintiffs and the Class, which would naturally result from Card Information theft.

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

86. In addition, in the years leading up to the Chipotle Data Breach and during the course of the breach itself and the investigation that followed, Chipotle failed to follow the guidelines set forth by the FTC. Indeed, Julie Conroy – research director at the research and advisory firm Aite Group – has identified that "If your data was stolen through a data breach that means you were somewhere out of compliance."[16]

E. Plaintiffs and Class Members Suffered Damages and Are at Risk of Further Harm

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

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

[16] http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited Oct. 24, 2017).

resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

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

90. The information Defendant compromised, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[17] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

91. 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

[17] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* <http://www.lagunawoodsvillage.com/images/lwlagunawoods/Fighting%20back%20Against%20Identity%20Theft.pdf> (last visited Oct. 24, 2017).

get medical treatment on your health insurance."[18]

92. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[19] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

93. Identity thieves can use personal information such as that of Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, the information stolen from Chipotle's computers can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.[20]

94. Identity thieves may also commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

95. In addition, identity thieves may get medical services using consumers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an

---

[18] FTC, Warning Signs of Identity Theft, *available at* <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited Oct. 24, 2017).

[19] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/276> (last visited Oct. 24, 2017) (the "2013 Identity Fraud Report").

[20] *Id.*

arrest.

96. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[21] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

97. Even if credit card companies may be responsible for some of the unauthorized transactions, consumers affected by the Chipotle Data Breach may be liable for up to $50 of fraudulent charges.[22]

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

99. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[23]

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

101. There may be a time lag between when harm occurs versus when it is discovered, and also between when Card Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a

[21] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Oct. 24, 2017).
[22] http://www.whec.com/news/restaurants-exposed-local-couple-chipotle-breach/4500701/ (last visited Oct. 24, 2017).
[23] *See* 2013 Identity Fraud Report.

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.[24]

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

- contact the three major credit bureaus;
- contact the FTC;
- place fraud alerts on credit files; and
- place security freezes on credit files; [25] [26]

103. Notwithstanding Defendant's wrongful actions and inaction and the

---

[24] GAO, Report to Congressional Requesters, at p.33 (June 2007), *available at* <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Oct. 24, 2017).

[25] *See* https://www.engadget.com/2017/05/26/chipotle-hack-stole-credit-card-information-us-march-april/ (last visited Oct. 24, 2017) (". . . Chipotle is not offering credit monitoring services to compromised customers.").

[26] *See* https://www.chipotle.com/security (last visited Oct. 24, 2017).

resulting Data Breach, Defendant has not offered consumers any credit monitoring and identity theft protection services, instead merely directing customers how to obtain credit reports and implement fraud alerts and security freezes.[27] This response is insufficient because, *inter alia*, it does not address many categories of damages being sought. The cost of adequate and appropriate mitigation, such as coverage or insurance, against the loss position Defendant has placed Plaintiffs and Class members in, is ascertainable and is a determination appropriate for the trier of fact.

104. Chipotle's failure to adequately protect consumers' Card Information has resulted in consumers having to undertake these errands that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of sums of money, while Chipotle is not doing anything to assist those affected by the data breach. Instead, as one source identified, Chipotle is putting the burden on the consumer to discover possible fraudulent transactions.[28]

CLASS ALLEGATIONS

105. Plaintiffs bring this action on behalf of themselves and the following Class pursuant to FED. R. CIV. P. 23:

> All persons residing in the United States who made a credit or debit card purchase at any Chipotle or Pizzeria Locale location affected by the Chipotle Data Breach between March 24, 2017 and April 18, 2017.

106. Plaintiffs also define three subclasses as follows:

[27] https://www.chipotle.com/security (last visited Oct. 24, 2017).
[28] http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited Oct. 24, 2017).

Arizona Class:

All persons who made a credit or debit card purchase at any Chipotle or Pizzeria Locale location in Arizona affected by the Chipotle Data Breach between March 24, 2017 and April 18, 2017.

California Class:

All persons who made a credit or debit card purchase at any Chipotle or Pizzeria Locale location in California affected by the Chipotle Data Breach between March 24, 2017 and April 18, 2017.

Illinois Class:

All persons who made a credit or debit card purchase at any Chipotle or Pizzeria Locale location in Illinois affected by the Chipotle Data Breach between March 24, 2017 and April 18, 2017.

Missouri Class:

All persons who made a credit or debit card purchase at any Chipotle or Pizzeria Locale location in Missouri affected by the Chipotle Data Breach between March 24, 2017 and April 18, 2017.

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

108. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many thousands of members who are geographically dispersed. As noted above, a spokesperson for Chipotle has

acknowledged that "most" of its stores were affected by the breach.

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

110. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class-action litigation; and Plaintiffs and their counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

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

of the case. By contrast, the class-action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

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

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

- whether Chipotle engaged in the wrongful conduct alleged herein;
- whether Chipotle owed a duty to Plaintiffs and members of the Class to adequately protect their Card Information and to provide timely and accurate notice of the data breach to Plaintiffs and the Class;
- whether Chipotle breached its duty to Plaintiffs and the Class by failing to provide timely and accurate notice to Plaintiffs and the Class about the breach;
- whether Chipotle breached duties owed to Plaintiffs and the Class by failing to provide adequate data security;
- whether Chipotle violated federal and state laws, thereby breaching its duties to Plaintiffs and the Class;

- whether Chipotle knew or should have known that its computer and network systems were vulnerable to attack from hackers;
- whether Chipotle's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems, resulting in the loss of customers' Card Information;
- whether Chipotle wrongfully failed to inform Plaintiffs and members of the Class that it did not maintain computer software and other security procedures sufficient to reasonably safeguard consumer financial and personal data; and whether Chipotle failed to inform Plaintiffs and the Class of the data breach in a timely and accurate manner;
- whether Chipotle wrongfully waited to inform Plaintiffs and Class members that their sensitive financial and personal information was exposed in the security breach;
- whether Chipotle continues to breach duties to Plaintiffs and Class members and continues to fail to adequately protect sensitive Card Information and other financial information;
- whether Chipotle has sufficiently addressed, remedied, or protected Plaintiffs and Class members following the data breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class members will not experience further harm;
- whether Plaintiffs and members of the Class suffered injury as a proximate result of Chipotle's conduct or failure to act; and

- whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class.

114. The claims of the Class may be certified under Rule 23(b)(1), (b)(2) and/or (b)(3). The members of the Class seek declaratory and injunctive relief but also seek sizeable monetary relief.

115. 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 Defendants 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 failed to comply with its own policies and

applicable laws, regulations, and industry standards relating to data security;

f. 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;

g. 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;

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

i. Whether Defendant breached the implied contract.

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

116. Plaintiffs reallege and incorporate all previous allegations.

117. Chipotle collected Card Information from Plaintiffs and Class Members in exchange for products and services.

118. Chipotle owed a duty to Plaintiffs and the Class to maintain confidentiality

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

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

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

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

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

of Plaintiffs and Class members.

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

124. Chipotle breached the duties it owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiffs and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and Class members.

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

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

126. Plaintiffs reallege and incorporate all previous allegations.

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

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice

by businesses, such as Chipotle, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Chipotle's duty.

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

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

131. Chipotle had a duty to Plaintiffs and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' personal information.

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

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

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

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

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

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

COUNT III
Violation of Colorado Consumer Protection Act,
COLO. REV. STAT. § 6-1-105(1)(l), *et seq.*
(On behalf of Plaintiffs and the Class)

138. Plaintiffs reallege and incorporate all previous allegations.

139. 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.

140. 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.

141. 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.

142. 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.

143. 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.

144. 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.

145. 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.

146. 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.

147. As alleged herein 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: i) failing to maintain adequate computer systems and data security practices to safeguard customers' Card Information; ii) failing to disclose that its computer systems would not adequately protect and safeguard Card Information; and, iii) accepting credit and debit card payments after it knew or should have known of the Data Breach and before it remedied the Breach.

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

a. omitting and/or misrepresenting 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. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

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

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

f. 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.

149. 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.

150. 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, but are not limited to: unauthorized charges on their debit and credit card accounts; theft of their personal and financial information by criminals; costs associated with the detection and prevention of identity theft; costs associated with unauthorized use of their financial accounts; costs associated with the cancellation and re-issuing of

payment cards; 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; lost value of benefits from use of payment cards; lost time associated with handling the administrative consequences of the data breach; 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; impairment to their credit scores and ability to borrow and/or obtain credit; and, the continued risk to their personal information, which remains on Chipotle's insufficiently secured computer systems.

151. 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's 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.

152. 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 IV
Breach of Implied Contract
(Individually and on Behalf of the Class)

153. Plaintiffs reallege and incorporate all previous allegations.

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

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

156. Plaintiffs and Class Members paid money to Chipotle and, in connection with those transactions, provided Chipotle with their Card Information. In exchange, Chipotle agreed, among other things: (1) to provide food products to Plaintiffs and Class Members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Card Information; (3) to protect Plaintiffs' and Class Members' personal information in compliance with federal and state laws and regulations and industry standards, and (4) to accurately and promptly notify Plaintiffs and Class Members if their data had been breached or compromised.

157. Protection of personal information is a material term of the contracts between Plaintiffs and Class Members, on the one hand, and Chipotle, on the other hand. Had Plaintiffs and Class Members known that Chipotle does not adequately protect

customer Card Information, they would have never made purchases at Chipotle.

158. Chipotle did not satisfy its promises and obligations to Plaintiffs and Class Members under the contracts in that it did not take reasonable measures to keep Plaintiffs' and Class Members' personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards. Chipotle materially breached its contracts with Plaintiffs and Class Members by failing to implement adequate payment card and Card Information security measures.

159. Chipotle further breached its contracts with Plaintiffs and Class Members by failing to provide timely and accurate notice to them that their Card Information was compromised in and as a result of the Data Breach.

160. Plaintiffs and Class Members fully performed their obligations under their contracts with Chipotle.

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

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

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

164. Accordingly, Plaintiffs and Class Members have been injured as a proximate result of Chipotle's breaches of contract, sustained actual losses and damages as described above, and are entitled to damages and/or restitution in an amount to be proven at trial.

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

165. Plaintiffs reallege and incorporate all previous allegations.

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

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

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

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

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

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

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

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

173. Plaintiff Gordon realleges and incorporates all previous allegations.

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

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

Id. § 44-1522.

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

"sale" of "merchandise" as defined by ARIZ. REV. STAT. § 44-1521(7).

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

- failing to maintain sufficient security to keep Plaintiff Gordon's and Class Members' sensitive Card Information being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of food and food services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Card Information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with sale of food and food services, by representing that Chipotle did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' Card Information; and
- failing to take proper action following the data breach to enact adequate privacy and security measures and protect Class Members' Card Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

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

and Class members' ordinary, foreseeable and reasonable expectations concerning the security of their Card Information on Chipotle's computer servers.

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

179. Chipotle also engaged in unfair acts and practices, in connection with the sale of services by failing to maintain the privacy and security of Class Members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

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

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

182. As a result of Chipotle's wrongful conduct, Plaintiff Gordon and Class members were injured in that they never would have allowed their sensitive Card

Information – the value of which Plaintiff Gordon and Class members no longer have control – to be provided to Chipotle if they had been told or knew that Chipotle failed to maintain sufficient security to keep such data from being hacked and taken by others.

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

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

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

COUNT VII
Violation of the California Customer Records Act
CAL. CIV. CODE § 1798.80, *et seq.*
(By Plaintiffs Baker and Conard and the Mercer Plaintiffs, Individually and on Behalf of the California Class)

186. Plaintiffs Baker and Conard and the Mercer Plaintiffs incorporate all foregoing substantive allegations as if fully set forth herein.

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

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

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

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

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

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

193. Plaintiffs Baker and Conard and the Mercer Plaintiffs accordingly request that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored customer data; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems; (7) ordering that Defendant purge, delete, and destroy in a reasonable secure manner customer data not necessary

for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who purchase Defendant's food through the internet; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their PII/PCD to third parties, as well as the steps Defendant's customers must take to protect themselves.

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

COUNT VIII
Violation of the California Unfair Competition Law
CAL. BUS. & PROF. CODE § 17200, *et seq.*
(By Plaintiffs Baker and Conard and the Mercer Plaintiffs, Individually and on Behalf of the California Class)

195. Plaintiffs Baker and Conard and the Mercer Plaintiffs incorporate all foregoing substantive allegations as if fully set forth herein.

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

197. Plaintiffs Baker and Conard and the Mercer Plaintiffs suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

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

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

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

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

202. Defendant's conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, CAL. CIV. CODE § 1798, *et seq.*, and the CRA concerning customer records—which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable

security measures.

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

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

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

206. As a result of Defendant's violations of the UCL, Plaintiff Baker, Plaintiff Conard, the Mercer Plaintiffs, and Class members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored customer data;

(2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems; (7) ordering that Defendant purge, delete, and destroy in a reasonable secure manner customer data not necessary for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who purchase Defendant's food through the internet; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their PII to third parties and the theft of Defendant's source code, as well as

the steps Defendant's customers must take to protect themselves.

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

COUNT IX
Violation of the California Consumers Legal Remedies Act
CAL. CIV. CODE §§ 1750, *et seq.* ("CLRA")
(By Plaintiff Baker, Plaintiff Conard, and the Mercer Plaintiffs, Individually and on Behalf of the California Class)

208. Plaintiffs Baker and Conard and the Mercer Plaintiffs incorporate all foregoing substantive allegations as if fully set forth herein.

209. The CLRA proscribes "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale of goods or services to any consumer."

210. Chipotle is a "person" within the meaning of the CLRA. CAL. CIV. CODE §§ 1761(c).

211. Chipotle provides "services", sells "goods", and offers "services furnished in connection with the sale . . . of goods" within the meaning of the CLRA. CAL. CIV. CODE §§ 1761(a), (b).

212. Plaintiffs and members of the Class are "consumers" within the meaning of the CLRA. CAL. CIV. CODE §§ 1761(d).

213. Plaintiffs and Class members engaged in "transactions" with Chipotle within the meaning of the CLRA. CAL. CIV. CODE §§ 1761(e).

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

- failing to maintain sufficient security to keep Plaintiffs' and Class members' confidential and sensitive financial information from being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of food and providing food-related services, by representing that Chipotle would maintain adequate data privacy and security practices and procedures to safeguard Class members' personal information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with the sale of food and providing food-related services, by representing that Chipotle did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members' personal information;
- failing to prevent the Data Breach and promptly notify consumers thereof, and violating CAL. CIV. CODE § 1798.80, *et seq.*; and
- failing to take proper action following the data breach to make victims of the Data Breach whole and enact adequate privacy and security measures and protect Class members' personal information from further unauthorized disclosure, release, data breaches, and theft.

215. In addition, Chipotle's failure to disclose that its computer systems were not well-protected (*i.e.*, that its security systems lagged behind the standard for other point of sale merchants by failing to incorporate chip technology) and that Plaintiffs' and Class

members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Chipotle knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and the Class; and (b) defeat Plaintiffs' and Class members' ordinary, foreseeable and reasonable expectations concerning the security of Chipotle's computer servers.

216. Defendant intended that Plaintiff Baker, Plaintiff Conard, the Mercer Plaintiffs, and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Chipotle's offering of food and food-related services and incorporating Plaintiffs' and Class members' sensitive information on its computer servers, in violation of the CLRA.

217. Chipotle also engaged in unfair acts and practices, in connection with the sale of food and food-related services by failing to maintain the privacy and security of Class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), and the California Customer Records Act (CAL. CIV. CODE § 1798.80, *et seq.*).

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

219. Chipotle's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Chipotle that applied to all Class members and were repeated continuously before and

after Chipotle obtained confidential financial and personal data concerning Plaintiffs and Class members. All Class members have been adversely affected by Chipotle's conduct and the public was and is at risk as a result thereof.

220. As a result of Chipotle's wrongful conduct, Plaintiff Baker, Plaintiff Conard, the Mercer Plaintiffs, and Class members were injured in their business or property in that they never would have allowed their sensitive and personal data – property that they have now lost – to be provided to Chipotle if they had been told or knew that Chipotle failed to maintain sufficient security to keep such data from being hacked and taken by others.

221. Chipotle's unfair and/or deceptive conduct proximately caused Plaintiffs' and Class members' injuries because, had Chipotle maintained the sensitive information with adequate security, Plaintiffs and the Class members would not have lost it.

222. Chipotle knew, should have known, or was reckless in its conduct and failure to keep Plaintiffs' and Class members' private information secure.

223. Plaintiff Baker and the Mercer Plaintiffs sent a demand letter to Defendant *via* certified mail pursuant to the requirements of the CLRA on July 7, 2017, providing the notice required by CAL. CIV. CODE § 1782(a).

224. Plaintiffs seek monetary damages against Defendant pursuant to CAL. CIV. CODE §§ 1781 and 1782, as well as an order awarding costs of court and attorneys' fees under CAL. CIV. CODE § 1780(e).

COUNT X
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILL. COMP. STAT. §§ 505/1, *et seq.* ("Illinois CFA")
(By Plaintiff Fowler Individually and on Behalf of the Illinois Class)

225. Plaintiffs incorporate all foregoing substantive allegations as if fully set forth herein.

226. This claim is brought on behalf of Plaintiff Fowler and the Illinois Class.

227. Plaintiff and the Illinois Class are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e). Plaintiff, the Class, and Chipotle are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

228. Chipotle is engaged in "trade" or "commerce", including provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

229. Chipotle engages in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

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

- failing to maintain sufficient security to keep Plaintiff Fowler's and Class Members' sensitive Card Information being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of food and food services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Card Information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with sale of food and food services, by representing that Chipotle did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' Card Information; and
- failing to take proper action following the data breach to enact adequate privacy and security measures and protect Class Members' Card Information and other personal information from

further unauthorized disclosure, release, data breaches, and theft.

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

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

233. Chipotle also engaged in unfair acts and practices, in connection with the sale of services by failing to maintain the privacy and security of Class Members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

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

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

236. Defendant also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et. seq.*, which provides, at Section 10:

> Notice of Breach.
>
> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

237. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

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

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

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

241. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff Fowler and the Class seek actual damages, compensatory, punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the Illinois CFA.

COUNT XI
Violations of the Illinois Uniform Deceptive Trade Practices Act
815 ILL. COMP. STAT. §§ 510/1, *et seq*. ("Illinois DTPA")
(By Plaintiff Fowler Individually and on Behalf of the Illinois Class)

242. Plaintiffs repeat and reallege the allegations above as if fully set forth herein.

243. This claim is brought on behalf of Plaintiff Fowler and the Illinois Class.

244. Plaintiff Fowler, the Class, and Chipotle are "persons" as defined in 815 ILL. COMP. STAT. § 510/1(5).

245. The Illinois DTPA broadly prohibits deceptive trade practices. As set forth herein, Chipotle failed to safeguard Plaintiff's and Class members' confidential and sensitive personal information. Accordingly, Chipotle has engaged in deceptive trade practices as defined in 815 ILL. COMP. STAT. § 510/2.

246. Chipotle's actions as set forth above occurred in the conduct of trade or commerce.

247. Chipotle knew or should have known that its conduct violated the Illinois DTPA.

248. Chipotle's conduct was material to Plaintiff and the Illinois Class.

249. As set forth herein, Plaintiff and the Illinois Class suffered ascertainable loss caused by Chipotle's violations of the Illinois DTPA, which proximately caused injuries to Plaintiff and the other Class members.

250. Pursuant to 815 ILL. COMP. STAT. § 510/3, Plaintiff and the Class are entitled to an award of injunctive relief to prevent Chipotle's deceptive trade practices and, because Chipotle's conduct was willful, an award of reasonable attorneys' fees.

COUNT XII
Violation of the Missouri Merchandising Practices Act
MO. ANN. STAT. § 407.020(1), *et seq.* ("MMPA")
(By Plaintiff Greg Lawson Individually and on Behalf of the Missouri Class)

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

252. This claim is brought on behalf of Plaintiff Lawson and the Missouri Class.

253. The MMPA provides in part:

> The act, …by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce … is declared to be an unlawful practice.
> MO. ANN. STAT. § 407.020.

254. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the PII and PCD of Plaintiff Lawson and the Missouri Class, Defendant violated the provisions of § 407.020 of the MMPA.

255. Chipotle's actions as set forth above occurred in the conduct of trade or commerce.

256. The acts and conduct of Defendant Chipotle as alleged above violated the MMPA by, among other things:

- failing to maintain sufficient security to keep confidential and sensitive financial information of Plaintiff Lawson and the Class from being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of food and providing food-related services, by representing that Chipotle would maintain adequate data privacy and security practices and procedures to safeguard Class members' personal information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with the sale of food and providing food-related services, by representing that Chipotle did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members' personal information; and,

- failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of Class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws.

257. Due to the Chipotle Data Breach, Plaintiff Lawson and the Missouri Class have lost property in the form of their Card Information and have suffered actual damages. Further, Defendant's failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of its customers has resulted in Plaintiff Lawson and the Class spending time and money to protect against identity theft. Plaintiff and the Class are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Defendant's practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

258. As a result of Defendant's practices, Plaintiff Lawson and the Missouri Class have suffered injury-in-fact and have lost money or property. As a result of Defendant's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff Lawson and members of the Missouri Class have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and

(b)(3), or alternatively pursuant to FED. R. CIV. P. 23(c)(4), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiffs as Class representatives and their counsel as Class counsel.

B. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

C. Award Plaintiffs and the Class appropriate equitable relief, including restitution, and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct, in an amount to be determined.

D. Award Plaintiffs and the Class injunctive and declaratory relief as may be appropriate. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information; cure any deficient, incomplete, or inaccurate disclosures by Chipotle to Plaintiffs and the Class regarding the Chipotle Data Breach; and extend credit monitoring services and services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

E. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

F. Award Plaintiffs and the Class reasonable attorneys' fees and costs as allowable.

G. Award Plaintiffs and the Class such other favorable relief as allowable under

law or at equity.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury for all issues so triable under the law.

Dated: December 8, 2017

Respectfully submitted,

/s Kevin S. Hannon
Kevin S. Hannon
THE HANNON LAW FIRM, LLC
1641 Downing Street
Denver, Colorado 80218
Tel: 303-861-8800
khannon@hannonlaw.com
Benjamin F. Johns
Andrew W. Ferich
Jessica L. Titler
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
bfj@chimicles.com
awf@chimicles.com
jlt@chimicles.com

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

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

Christopher D. Jennings
JOHNSON VINES PLLC
2226 Cottondale Lane, Suite 210
Little Rock, Arkansas 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

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I, Kevin S. Hannon, hereby certify that on December 8, 2017, I filed a true and correct copy of the above document with the Clerk of the Court in accordance with the Court's Rules on Electronic Service, which caused notification of filing to be sent to all counsel of record.

/s/ Kevin S. Hannon
Kevin S. Hannon