UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

BELLWETHER COMMUNITY CREDIT UNION and ALCOA COMMUNITY FEDERAL CREDIT UNION, on behalf of themselves and all others similarly situated, Plaintiff, v. CHIPOTLE MEXICAN GRILL, INC., Defendant.	Case No. 1:17-cv-1102-WJM-STV **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Bellwether Community Credit Union and Alcoa Community Federal Credit Union ("Plaintiffs"), through their undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, file this Consolidated Amended Class Action Complaint against Defendant Chipotle Mexican Grill, Inc. ("Chipotle" or "Defendant") and state the following:

INTRODUCTION

1. This is a class action on behalf of financial institutions that suffered, and continue to suffer, property damage and financial losses as a result of Chipotle's implementation of inadequate measures to protect Plaintiffs' and other financial institutions' payment card data from being stolen from Chipotle's point-of-sale ("POS") and computer systems. From approximately March 24, 2017 to April 18, 2017, Chipotle allowed a computer hacker to enter Chipotle's computer system undetected and install malware that infected POS systems at more than 2,200 of Chipotle's U.S. restaurants in 47 states (the "Data Breach"). The malware enabled the hacker to steal the cardholder names, credit and debit card numbers, card expiration dates,

card verification values, service codes, and other information (collectively, "Payment Card Data") of customers using payment cards issued by Plaintiffs and the Class (defined below). The stolen Payment Card Data was then sold by the hacker and used by cyber-criminals to make fraudulent purchases.

2. This confidential Payment Card Data, which is owned by and is the property of Plaintiffs and the Class, was compromised and rendered useless because of Chipotle's affirmative acts in implementing data security measures that were inadequate to properly protect the Payment Card Data that Plaintiffs and the Class entrusted to Chipotle. Chipotle, by accepting payment cards at its restaurants, knew or should have known it was required to adequately protect Payment Card Data.

3. The susceptibility of POS systems to malware is well known throughout the retail and restaurant industries. Indeed, Chipotle is well aware of the risks, as it was subject to a data breach in 2004. In the last five years, malware placed on POS systems caused practically every major data breach involving retail stores or fast-food chains, resulting in millions of compromised payment cards.

4. Despite the susceptibility of POS systems to hacking, a data breach that compromises sensitive payment card information is not an inevitability of doing business; rather, numerous measures can be taken to prevent intrusion by unauthorized personnel into POS devices and networks and to limit the effect of an intrusion if it occurs. For example, one data security expert recommends a "Tripod of POS Security," comprised of the following protective measures: (1) POS systems that support EMV chip-based payment cards (a highly secure method of transmitting credit card data that replaces the traditional magnetic stripe); (2) end-to-end

encryption, which encrypts Payment Card Data as soon as payment cards are swiped; and (3) tokenization, which replaces credit and debit card numbers with a meaningless series of letters and numbers, rendering any information collected by hackers useless.[1]

5. Another data security expert commented that "POS systems are not difficult to secure if merchants would simply follow the advice that has been put out by [industry experts]. Most of the advice is based on security best practices ***that have been around for years***. Unfortunately, it often takes a data breach for companies to have their eyes opened to the impact their negligence can have[.]"[2] [Emphasis added.]

6. Despite the well-publicized and ever-growing threat of cyber-attacks targeting Payment Card Data through vulnerable POS systems and inadequately protected computer networks, Chipotle took inadequate measures to prevent or detect the Data Breach, as the hacker launched its malicious payloads and ultimately exfiltrated Payment Card Data from Chipotle's computer network. Chipotle knowingly refused to implement certain best practices, understaffed its IT department, chose not to upgrade critical security systems, used an outdated POS system that no longer was supported by the hardware and software manufacturers, ignored explicit warnings about the vulnerability of its POS system, and disregarded and/or violated applicable industry standards.

---

[1] Point of sale security: Retail data breaches at a glance, DATACAP SYSTEMS, INC. (May 12, 2016), https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#.

[2] John H. Sawyer, *Tech Insight Defending Point-Of-Sale Systems*, DARKREADING (Jan. 24, 2014), https://www.darkreading.com/attacks-breaches/tech-insight-defending-point-of-sale-systems/d/d-id/1141214.

7. Plaintiffs and the Class have suffered property damage – *i.e.*, the complete and immediate obsolescence of their computer data associated with the compromised payment cards – and other financial losses as a result of the Data Breach. Specifically, Plaintiffs and other financial institutions have been forced to: (a) replace the computer data rendered useless by the Data Breach; (b) cancel or reissue any credit and debit cards affected by the Data Breach; (c) close any deposit, transaction, checking, or other accounts affected by the Data Breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (d) refund any cardholder for any unauthorized transaction relating to the Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts.

8. This class action is brought on behalf of financial institutions throughout the U.S. to recover the damages that they and others similarly situated have suffered, and continue to suffer, as a direct result of the Data Breach. Plaintiffs assert claims for negligence, negligence *per se*, violation of state consumer protection statutes, misappropriation of trade secrets in violation of the Defend Trade Secrets Act of 2016 ("DTSA"), 18 U.S.C. § 1831, *et seq*., and declaratory and ancillary equitable relief.

PARTIES

9. Plaintiff Bellwether Community Credit Union ("Plaintiff Bellwether") is a credit union headquartered at 425 Hooksett Road, Manchester, New Hampshire 03104. Plaintiff Bellwether employs numerous methods to maintain the confidentiality of its Payment Card Data and to prevent disclosure of its Payment Card Data to unauthorized third parties. As a result of the Chipotle Data Breach, Plaintiff Bellwether has suffered, and continues to suffer, injuries,

including, *inter alia*, property damage to the computer data associated with the Payment Card Data rendered useless as a result of the Data Breach, as well as costs to: (a) replace the computer data rendered useless by the Data Breach; (b) cancel or reissue any payment cards affected by the Data Breach; (c) close any deposit, transaction, checking, or other accounts affected by the Data Breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (d) refund any cardholder for any unauthorized transaction relating to the Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts. Specifically, Plaintiff Bellwether has reissued payment cards impacted by the Data Breach for members who are located in the following states: California, Florida, Maine, Massachusetts, New Hampshire, Virginia, Vermont, and Wisconsin. Plaintiff Bellwether, thus, has suffered injury in each of these states. Plaintiff Bellwether is subject to an imminent threat of future harm because Chipotle's response to past data breaches has been so inadequate that it is doubtful that it has cured the deficiencies in its data security measures sufficiently to prevent a subsequent data breach.

10. Plaintiff Alcoa Community Federal Credit Union ("Plaintiff Alcoa") is a credit union headquartered at 1125 Military Rd., Benton, Arkansas 72015. Plaintiff Alcoa employs numerous methods to maintain the confidentiality of its Payment Card Data and to prevent disclosure of its Payment Card Data to unauthorized third parties. As a result of the Chipotle Data Breach, Plaintiff Alcoa has suffered, and continues to suffer, injuries, including, *inter alia*, property damage to the computer data associated with the Payment Card Data rendered useless as a result of the Data Breach, as well as costs to: (a) replace the computer data rendered useless by the Data Breach; (b) cancel or reissue any payment cards affected by the Data Breach; (c)

close any deposit, transaction, checking, or other accounts affected by the Data Breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (d) refund any cardholder for any unauthorized transaction relating to the Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts. Specifically, Plaintiff Alcoa has reissued debit cards impacted by the Data Breach for members who reside in Arkansas. Plaintiff Alcoa, thus, has suffered injury in Arkansas. Plaintiff Alcoa is subject to an imminent threat of future harm because Chipotle's response to past data breaches has been so inadequate that it is doubtful that it has cured the deficiencies in its data security measures sufficiently to prevent a subsequent data breach.

11. Defendant Chipotle Mexican Grill, Inc. is a Delaware corporation with a principal executive office located at 1401 Wynkoop St., Suite 500, Denver, Colorado 80202. Chipotle operates a chain of fast-casual restaurants that serve "a focused menu of burritos, tacos, burrito bowls and salads, made using fresh, high-quality ingredients." As of March 31, 2017, Chipotle operates approximately 2,249 restaurants throughout the United States. In 2016, its revenues totaled approximately $3.9 billion.

JURISDICTION AND VENUE

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

citizen of Delaware, where it is incorporated, and Colorado, where its principal place of business is located.

13. This Court also has federal subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs assert a claim under the DTSA, 18 U.S.C. § 1832. The Court also has supplemental or pendant jurisdiction over Plaintiffs' remaining claims insofar as those claims form part of the same case or controversy as the federal question claim, pursuant to 28 U.S.C. § 1367.

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

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

FACTUAL BACKGROUND

A. Chipotle Had a Common Law Duty to Protect Payment Card Data in Light of the Foreseeability of the Risk It Created by Knowingly Implementing Inadequate Data Security Measures

16. Plaintiffs and the Class are financial institutions that issue payment cards, such as credit and debit cards, to their customers.

17. Chipotle restaurants accept payment cards for the purchase of goods and services. In fact, according to Chipotle, 70% of its sales are attributable to credit and debit card transactions. In processing payment card transactions through its POS system, Chipotle acquires a substantial amount of Payment Card Data.

18. A POS system is an on-site device that manages both cash and payment card transactions from consumer purchases. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[3] Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory. *Id*. at 5. Any time that Payment Card Data is "in the clear"—that is, in plain text format that is readable by a person or computer—it is extremely vulnerable to theft. It is this unencrypted Payment Card Data on the POS system that hackers seek to access.

19. It is well known that Payment Card Data has considerable value to and often is targeted by hackers, who easily can sell Payment Card Data, as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[4] Tim Erlin, Vice President of Tripwire, a threat, security and compliance solutions vendor, noted that "[a]s long as compromised credit card data continues to be a valuable commodity on the black market, any company collecting or processing valid credit card information will continue to be a high value target."[5] Intruders with access to Payment Card

---

[3] *A Special Report on Attacks on point-of-sales systems* at 6, Symantec (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf.

[4] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016, 10:47 AM), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[5] Dan Rayward, *Chipotle Reports Suspicious Activity on POS System*, INFOSECURITY MAGAZINE (Apr. 26, 2017), https://www.infosecurity-magazine.com/news/chipotle-suspicious-activity-pos/.

Data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[6]

20. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including Arby's, Wendy's, Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, Kmart, and many others.

21. Each of these massive data breaches involved malware placed on each merchant's POS system. For example, in 2013, hackers infiltrated Target's POS system, stealing information from an estimated 40 million payment cards in the United States.[7] In 2014, over 7,500 self-checkout POS terminals at Home Depot locations throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[8] In 2016, on-site POS systems at more than 1,000 Wendy's restaurants were infiltrated with malware, resulting in the theft of Payment Card Data for nearly six months.[9]

22. Despite the well-known vulnerabilities of POS systems, available security measures and business practices would have significantly reduced or eliminated hackers' ability

---

6 *A Special Report*, *supra* n.3.

7 Brett Hawkins, *Case Study: The Home Depot Data Breach* at 3-4, SANS INSTITUTE (Jan. 2015), https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367.

8 *Id.* at 4, 7.

9 Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KREBSONSECURITY (July 8, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/.

to successfully infiltrate merchants' POS systems. One report indicated that over 90% of the data breaches occurring in 2014 were preventable.[10]

23. As discussed fully below, the payment card networks (MasterCard, Visa, Discover, and American Express), data security organizations, federal agencies, and state governments have implemented recommended standards of care regarding security measures designed to prevent these types of intrusions into POS systems. Chipotle's adherence to reasonable standards of care could have either prevented or timely detected this Data Breach.

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

25. Chipotle is, and at all relevant times was, fully aware of the significant volume of daily payment card transactions at Chipotle's restaurants, amounting to tens of thousands of daily payment card transactions, and thus, the significant number of payment cards that would be impacted by a breach of Chipotle's POS systems.

26. Chipotle is, and at all relevant times has been, aware of the importance of safeguarding Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, including the significant harm that Plaintiffs and the Class

[10] *2016 Data Breach Investigations Report* at 1, VERIZON (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-Data-Security_en_xg.pdf.

would suffer. Indeed, in a notice relating to the Data Breach, Chipotle advised that "[i]f anyone sees an unauthorized charge, they should immediately notify the bank that issued the card."[11]

27. Despite that Chipotle understood the risk that it created in leaving its POS systems vulnerable to a malware attack, Chipotle took unreasonable and insufficient measures to protect Payment Card Data by choosing not to employ widely available resources to prevent or detect an intrusion.

B. The Chipotle Data Breach

28. On April 25, 2017, Defendant issued a security notice announcing the Data Breach:

> We want to make our customers aware that we recently detected unauthorized activity on the network that supports payment processing for purchases made in our restaurants. We immediately began an investigation with the help of leading cyber security firms, law enforcement, and our payment processor. We believe actions we have taken have stopped the unauthorized activity, and we have implemented additional security enhancements. Our investigation is focused on card transactions in our restaurants that occurred from March 24, 2017 through April 18, 2017. Because our investigation is continuing, complete findings are not available and it is too early to provide further details on the investigation. We anticipate providing notification to any affected customers as we get further clarity about the specific timeframes and restaurant locations that may have been affected.
>
> Consistent with good practices, consumers should closely monitor their payment card statements. If anyone sees an unauthorized charge, they should immediately notify the bank that issued the card. Payment card network rules generally state that cardholders are not responsible for such charges.[12]

---

[11] *Notice of Data Security Incident*, CHIPOTLE MEXICAN GRILL, (last updated April 25, 2017), https://web.archive.org/web/20170506052230/http://www.chipotle.com/security (accessed by searching for Chipotle's security notice in the Internet Archive index).

[12] *Id.*

29. On April 27, 2017, MasterCard issued an Account Data Compromise ("ADC") Notification regarding the Data Breach to financial institutions, which indicated that Chipotle locations throughout the United States were impacted, that the estimated at-risk time frame was March 24, 2017 through April 18, 2017, and that full magnetic stripe Payment Card Data was compromised.

30. On April 28, 2017, Visa issued a Compromised Account Management System ("CAMS") alert regarding the Data Breach to financial institutions, which indicated that the estimated fraud "exposure window" for the Data Breach ran from March 24, 2017 to April 18, 2017. The CAMS alert further indicated that both Track 1 and Track 2[13] Payment Card Data may have been compromised in the Data Breach.

31. On May 26, 2017, Chipotle issued a second press release at the conclusion of its investigation, explaining:

> The investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Chipotle and Pizzeria Locale restaurants between March 24, 2017 and April 18, 2017. The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS device. . . .
>
> During the investigation, Chipotle removed the malware and continues to work with cyber security firms to evaluate ways to enhance its security measures. In addition, Chipotle continues to support law enforcement's investigation and is

[13] Track 1 Payment Card Data refers to cardholder name, primary account number, expiration date, card verification value/code, and service code; Track 2 Payment Card Data refers to primary account number, expiration date, card verification value/code, and service code.

working with the payment card networks ***so that the banks that issue payment cards can be made aware and initiate heightened monitoring***.[14]

32. [redacted]

33. [redacted]

[14] Press Release, *Chipotle Mexican Grill Reports Findings from Investigation of Payment Card Security Incident* (May 26, 2017), http://ir.chipotle.com/phoenix.zhtml?c=194775&p=irol-newsArticle&ID=2276953.

[redacted]

34. [redacted]

[redacted]

35. [redacted]

[redacted]

36. [redacted]

[redacted]

[15] A RAM scraping attack focuses on the POS terminal's memory, called random access memory ("RAM"), during the brief period of time when the terminal communicates Payment Card Data to the back-end system.

37. [redacted]

38. [redacted]

39. Chipotle's data security systems suffered from many deficiencies that made them susceptible to hackers. Chipotle knowingly:

a. ignored well-known data security risks, thereby intentionally allowing data security deficiencies to persist;

b. disregarded warnings that its Aloha POS system was incompatible with the antivirus software, causing frequent system crashes;

c. refused to upgrade the POS system when the manufacturer ceased providing security or technical updates for the POS operating system, which made the POS system highly vulnerable to attack;

d. lacked adequate firewall protection and proper network segmentation, which would have prevented hackers from accessing Payment Card Data;

e. refused to implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its POS and other systems that accessed Payment Card Data and otherwise would have protected Payment Card Data;

f. failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of the hacker and prevented Payment Card Data from being stolen; and

g. chose not to implement EMV technology for use with its POS systems, which would have provided complete protection for Payment Card Data.

C. Chipotle Breached Its Duty to Avoid Causing Plaintiffs and the Class Foreseeable Harm by Consciously Disregarding Known Risks

1. Despite Well-Known Risks, Chipotle's Lackadaisical Approach to Data Security Allowed Deficiencies to Persist

40. Much of the blame for the state of Chipotle's data security systems can be placed squarely on the shoulders of Chipotle's senior management, who knowingly failed to upgrade POS hardware and software and failed to maintain a system of accountability over data security. Indeed, Chipotle senior management were aware that many of the Company's POS terminals were outdated and used operating systems that the manufacturer no longer supported, which left Payment Card Data at risk of being compromised. Yet, Chipotle allowed these deficiencies to persist and failed to devote adequate resources to address security issues.

41. According to a former Chipotle IT Help Desk Specialist ("IT Help Desk Specialist"), the IT Help Desk was understaffed, overworked, and constantly overwhelmed and unable to effectively and timely handle outstanding requests. The IT Help Desk Specialist had voiced his concerns about the pervasive problems the IT Help Desk encountered to his supervisor, who was the IT Help Desk Manager.

42. The IT Help Desk Specialist also stated that Chipotle used outdated P1220 or P1230 Aloha POS terminals, which were "extremely old" models, in many of its stores. According to the IT Help Desk Specialist, it was Chipotle's approach to "let [each POS terminal] die, and then replace it." He stated that most Chipotle stores had two POS terminals; when one terminal crashed, an employee would have to travel to a nearby Chipotle location to pick up one of its functioning POS terminals.

43. Chipotle clearly was aware of the risk of a data breach occurring, as the IT Help Desk Specialist confirmed that in the 2015 and 2016 timeframe Chipotle had been subject to at least two phishing attacks where a store-level employee had clicked on a malicious email link that enabled attackers to spam all Chipotle personnel's emails. The IT Help Desk Specialist confirmed that these attacks, in turn, spread malicious spam throughout many of Chipotle's stores. The IT Help Desk Specialist explained that one month after the first attack, Chipotle was subject to a second phishing attack and, as a result, the IT Help Desk was "swamped" and "absolutely inundated with calls." The IT Help Desk Specialist stated that, when these phishing attacks occurred, the IT Help Desk "had no idea how to handle it" because there was no established protocol for how to deal with such an attack.

44. Chipotle also was aware of the threat of a data breach given the prior high-profile breaches that occurred at Target, Home Depot, Wendy's, and others. As early as October 2008, Visa issued a Data Security Alert describing the threat of RAM scraping malware.[16] In May 2009, Visa issued an updated Data Security Alert warning merchants that due to a memory parsing (RAM scraping) vulnerability "hackers are gaining unauthorized access to point-of-sale (POS) environments as a result of insecure remote desktop solutions or poor network configuration."[17] The May 2009 alert instructs companies to "secure their external and internal network perimeters to prevent unauthorized access to POS systems, payment processing servers, database servers or other servers where payment card data resides." *Id*. The May 2009 alert further instructs merchants to "secure your remote access connectivity," "implement a secure network configuration including egress and ingress filtering to only allow the ports/services necessary to conduct business" (i.e., segregate networks), "[m]onitor firewalls for suspicious traffic (particularly outbound traffic to unknown addresses)," "[i]mplement file integrity monitoring," "[s]ecure systems so that unauthorized software cannot be installed," "[e]nsure that all anti-virus and anti-spyware software programs are up-to-date," and "[r]outinely examine systems and networks for newly-added hardware devices; unknown files and software." *Id*.

---

[16] Numaan Huq, *2014 – An Explosion of Data Breaches and PoS RAM Scrapers*, Trend Micro: Trend Labs Security Intelligence Blog (Sept. 11, 2014, 2:16 AM), http://blog.trendmicro.com/trendlabs-security-intelligence/2014-an-explosion-of-data-breaches-and-pos-ram-scrapers/ (last accessed October 26, 2017).

[17] Visa Data Security Alert – *Targeted Hospitality Sector Vulnerabilities* (May 28, 2009), https://webcache.googleusercontent.com/search?q=cache:inr6SWDrgc8J:https://www.firstdata.com/downloads/partners/fd_gpm_notice_visa_security_alert_28may09_partnersupport.doc+&cd=8&hl=en&ct=clnk&gl=us.

45. Indeed, in August 2013, Visa warned merchants, including Chipotle, of malware targeting POS systems. Specifically, the alert, entitled "Retail Merchants Targeted by Memory-Parsing Malware," warned: "Since January 2013, Visa has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane."[18]

46. In February 2014, Visa again warned Chipotle and other merchants of the increased risks posed by malware designed to target POS systems in an update to its August 2013 security alert. Specifically, the February 2014 alert stated:

> Visa is issuing this alert to make clients aware of new malware information and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access. Visa highly recommends merchants implement these signatures on security solutions to detect a suspected breach. However, Visa recommends performing sufficient due diligence prior to implementing any block to avoid any inadvertent connectivity issues for legitimate access.[19]

47. In November 2015, Visa issued another security alert notifying Chipotle and other merchants of additional malware infections targeting and impacting merchants and restaurants. This alert specifically stated that a restaurant group had been targeted by this form of malware attack and that "infections started in August 2015 but appeared to increase dramatically in the

---

[18] Visa Data Security Alert, *Retail Merchants Targeted by Memory-Parsing Malware - UPDATE* (August 2013), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf.

[19] Visa Data Security Alert, *Retail Merchants Targeted by Memory-Parsing Malware - UPDATE* (Feb. 2014), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf.

middle of October 2015."[20] The security alert further stated that "Windows XP and Windows 7 (both 32 bit and 64 bit) are the primary operating systems infected." *Id.*

48. Defendant also received additional warnings regarding malware infiltration of POS systems from the U.S. Computer Emergency Readiness Team ("U.S. CERT"), a government unit within the Department of Homeland Security, which alerted retailers to the threat of POS malware in two separate alerts, on January 2, 2014 and on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware.[21]

49. Chipotle knew or should have known of the susceptibility of its POS systems and that a breach of its corporate network would permit intruders to install malware at its locations throughout the U.S., putting Plaintiffs' and the Class's Payment Card Data at risk. In its most recent Form 10-K filed with the U.S. Securities and Exchange Commission ("SEC"), it acknowledged the prevalence of data breaches among retailers and stated that it previously suffered a data beach in 2004. Chipotle therefore should have been aware of the need to have adequate data security systems in place.

50. Specifically, in 2004, Chipotle recorded charges of $4 million to establish a reserve for claims seeking reimbursement for fraudulent credit and debit card charges, in addition to $1.5 million of additional expenses. Chipotle only learned of the 2004 data breach when the merchant bank that processed Chipotle's payment card transactions notified it. In this

---

[20] Security Alert, Visa, *Update - Cybercriminals Targeting Point Of Sale Integrators* (Nov. 13, 2015), https://usa.visa.com/dam/VCOM/download/merchants/alert-pos-integrators.pdf.

[21] *See* U.S. CERT, *Alert (TA14-002A): Malware Targeting Point of Sale Systems* (Jan. 2, 2014) (revised Oct. 6, 2016), https://www.us-cert.gov/ncas/alerts/TA14-002A; U.S. CERT, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), www.us-cert.gov/ ncas/alerts/TA14-212A.

2004 data breach, hackers stole Track 2 data from Chipotle's systems, which includes the customer's name, card number, card expiration date, and card verification number. Chipotle further explained that in the 2004 data breach, the internet gateways on Defendant's computers in some stores may not have been fully secure at all times.[22]

51. Moreover, in its most recent Form 10-K, Chipotle identified a future data breach as risk factor that would negatively impact its business operations:

> 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.[23]

---

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

[23] *Id.*

52. Despite acknowledging such risks, Chipotle disregarded the potential danger of a data breach by failing to devote adequate resources to address security issues and failing to take adequate steps to implement reasonable data security measures to prevent or timely detect the Data Breach.

2. Chipotle Disregarded Warnings that Its Aloha POS System Was Vulnerable to a Data Breach

53. At the time of the Data Breach, Chipotle restaurants used the Aloha POS system, a third-party system developed by NCR Corp. ("NCR"), a global technology company.[24]

54. According to the IT Help Desk Specialist, POS system crashes, which occurred due to the age of the hardware, were a "major issue" that occurred regularly throughout 2015 and 2016. Indeed, according to NCR, it discontinued customer support for Chipotle's outdated P1220 and P1230 Aloha POS systems in approximately 2012.[25]

55. The IT Help Desk Specialist explained that Chipotle's most common IT issues related to the Aloha POS system due to the POS system's incompatibility with other IT programs such as the antivirus software, which caused system crashes and situations where the POS system would be unable to properly authorize transactions due to the loss of internet connectivity.

56. With regard to conflicts between the Aloha POS system and Chipotle's other IT systems, the IT Help Desk Specialist stated that POS system crashes were a pervasive problem

---

[24] *Hot Concept Chipotle sizzles with cutting-edge Aloha enterprise POS technology*, RETAIL IT INSIGHTS, https://www.retailitinsights.com/doc/hot-concept-chipotle-sizzles-with-cutting-edg-0001 (last accessed October 30, 2017).

[25] *Drivers and Patches, P1220 Drivers*, NCR, http://www5.ncr.com/support/support_drivers_patches_radiant.asp?Class=Hospitality/P1220_display (last modified May 23, 2013, 10:48 PM).

throughout all of Chipotle's stores. The conflict between the antivirus software and the Aloha POS system was so severe that when the POS system rebooted, the system would launch into "blue screen" mode and would be unable to connect to the back end of Chipotle's POS system that allowed the store to transmit Payment Card Data to Chipotle's corporate headquarters.

57. A former IT Support Manager ("IT Support Manager"), who worked for Chipotle in its Denver headquarters from October 2009 to August 2016, likewise confirmed that Chipotle's antivirus software caused the POS system to crash and become inoperative. The IT Support Manager stated that, when the POS system lost internet connectivity, the restaurants were required to run POS transactions in "spool down mode," which enabled transactions to be authorized offline until the restaurant in question could re-establish internet connectivity.

58. The shortcomings of the Aloha POS system were publicly well known by the time of the Data Breach. A July 18, 2014 *ComputerWorld* article explained that "Matt Oh, a senior malware researcher with HP, recently bought a single Aloha point-of-sale terminal" and found:

> an eye-opening mix of default passwords, at least one security flaw and a leftover database containing the names, addresses, Social Security numbers and phone numbers of employees who had access to the system. His findings have received a fair amount of attention due to the role of such systems in high-profile data breaches at retailers including Target, Neiman Marcus and Michaels.[26]

59. According to the report, Oh "also found a memory-related problem known as a 'heap overflow' within a component called the Aloha Durable Messaging Service, which shuttles

[26] Jeremy Kirk, *Aloha point-of-sale terminal, sold on eBay, yields security surprises*, COMPUTERWORLD (July 18, 2014, 6:15 AM (PST)), https://www.computerworld.com/article/2490184/cybercrime-hacking/aloha-point-of-sale-terminal--sold-on-ebay--yields-security-surprises.html.

information between front-end and back-end systems. If exploited, the heap overflow 'could provide an attacker with full system level control of the target system[.]'" *Id*.

60. Moreover, in 2009, several restaurants in the U.S. that suffered data breaches sued the vendor and distributor of their Aloha POS systems. The lawsuit alleged that the Aloha POS system was non-compliant with industry standards (known as PCI DSS, discussed *infra*) and that hackers "were able to install keyloggers and steal credit card numbers resulting in hundreds of customers becoming victims of identity theft."[27] In fact, this lawsuit noted that, in 2007, Visa warned the vendor and distributor that "the Aloha POS system unnecessarily stored sensitive cardholder data," making it non-compliant with PCI DSS and a vulnerable target for hackers. *Id.*

61. Similarly, in 2012, two Romanian hackers confessed that they had targeted over 150 Subway sandwich restaurants by breaking into Subway's Aloha POS system.[28]

62. Despite the known vulnerabilities of the outdated Aloha POS system, Chipotle chose not to upgrade its POS system.

3. Chipotle Operated Its POS Terminals on an Outdated, Unsupported Operating System that Was Susceptible to Data Breach

63. Chipotle further knew that its POS systems were at risk for a potential data breach because Aloha POS systems run on Windows XP, an outdated operating system.

---

[27] Angela Moscaritolo, *Breached restaurateurs suing point-of-sale provider*, SC MEDIA US (Dec. 2, 2009), http://www.scmagazine.com/breached-restaurateurs-suing-point-of-sale-provider/article/158892/.

[28] Adam Estes, *How Romanian Hackers Stole $10 Million From Subway Customers*, MOTHERBOARD.VICE.COM (Sept. 18, 2012, 12:30 PM) https://motherboard.vice.com/en_us/article/aeeq5b/how-two-guys-stole-10-million-from-subway-customers.

64. POS systems are vulnerable to malware attacks when required software updates are not downloaded and installed on a timely basis. U.S. CERT therefore recommends updating POS software applications.[29]

65. In October 2013, an article titled "The End of Windows XP Could be the End for Your POS System" warned Aloha POS system users that "[i]f you're using a terminal that's a few years old, such as Micros or Aloha, it might be time to upgrade your POS system."[30] The article pointed out that POS systems, like Aloha POS, that utilized Windows XP were outdated and no longer supported by Microsoft.

66. In 2014, Microsoft, Windows XP's manufacturer, discontinued security updates and technical support for XP. Indeed, Microsoft published a specific warning to customers who continued to utilize Windows XP:

> After April 8, 2014, Microsoft will no longer provide security updates or technical support for Windows XP. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. ***PCs running Windows XP after April 8, 2014, should not be considered to be protected***, and it is important that you migrate to a current supported operating system – such as Windows 10 – so you can receive regular security updates to protect their computer from malicious attacks.[31]

[Emphasis added].

67. The IT Help Desk Specialist and IT Support Manager confirmed that a majority of Chipotle's Aloha POS system ran on the Windows XP operating system. To the IT Help Desk Specialist's knowledge, there was no initiative to upgrade the POS operating system.

---

[29] U.S. CERT, *Alert (TA14-002A)*, *supra* n.21.

[30] *The End of Windows XP Could be the End for Your POS System*, REVEL SYSTEMS (Oct. 1, 2013), http://revelsystems.com/blog/2013/10/01/end-windows-xp-end-pos-system/.

[31] *Support for Windows XP ended*, MICROSOFT (Apr. 8, 2014), https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support.

68. Thus, Chipotle knew that its XP-based POS terminals were using outdated software, were no longer being protected from malware, and were beset with additional problems, yet Chipotle refused to upgrade its POS system.

4. Chipotle Lacked Adequate Firewall Protection and Appropriate Network Segmentation

69. Chipotle failed to maintain adequate firewall protection, which would have prevented its computer network from being breached by hackers. Indeed, Chipotle should have been aware of the PCI DSS requirements and the significant risks associated with a deficient firewall and that such deficiencies could lead to a data breach.

70. A firewall can prevent unauthorized access to, or from, a private network by screening out traffic from hackers, viruses, worms, or other types of malware specifically designed to compromise a POS system. U.S. CERT therefore recommends that firewalls should be used to protect POS systems from outside attacks.[32]

71. Similarly, a Visa Data Security Alert, issued in February 2014, warned merchants, such as Chipotle, that they should be vigilant with respect to their firewalls and firewall configuration. The February 2014 security alert informed merchants that they should:

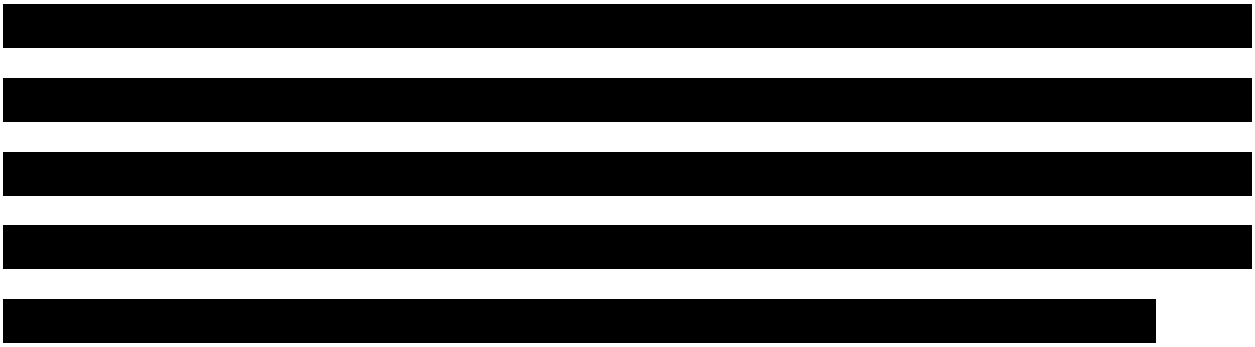
> [r]eview your firewall configuration and ensure only allowed ports, services and IP (internet protocol) addresses are communicating with your network. This is especially critical on outbound (e.g., egress) firewall rules, where compromised entities allow ports to communicate to any IP on the Internet. Hackers will leverage this misconfiguration to exfiltrate data to their IP address.[33]

72. Despite this, Chipotle failed to take necessary measures to maintain an adequate firewall that was properly configured to prevent hackers from penetrating its computer network.

---

[32] U.S. CERT, *Alert (TA14-002A), supra* n.21.

[33] Visa Data Security Alert (Feb. 2014), *supra* n.19.



73. In fact, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") has published a *Guide to Application Whitelisting* for computer security. The purpose of NIST and its Information Technology Laboratory includes the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. NIST states that the use of whitelisting "helps to stop the execution of malware, unlicensed software, and other unauthorized software."[34] NIST further recommends that "[o]rganizations should consider these technologies, particularly for centrally managed desktops, laptops, and servers, because of the relative ease in managing these solutions and the minimal additional cost. *Id.* at 5.

74. Indeed, the NIST Guide states that "application whitelisting software prevents installation and/or execution of any application that is not specifically authorized for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorized software." *Id.* at 2.

[34] Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, *NIST Special Publication 800-167: Guide to Application Whitelisting* at 3, NIST (Oct. 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

75. [redacted]

76. [redacted] As a result of this connectivity, and the lack of adequate firewall protection and appropriate network segmentation, a hacker not only could enter Chipotle's computer network, but also was able to jump unhindered between various network platforms and ultimately access Payment Card Data.

77. Chipotle knew or should have known firewalls and network segmentation were necessary, but chose to not comply with these minimum standards of care.

5. Chipotle Refused to Implement Protocols that Would Have Protected Payment Card Data

78. Chipotle failed to implement certain protocols, such as [redacted], and employing encryption and tokenization of Payment Card Data at the point of sale. These protocols would have detected and prevented unauthorized programs from being installed on Chipotle POS systems and otherwise would have protected Payment Card Data in the event of a data breach.

79. [redacted]

80. Radiant Systems, which is owned by NCR, the manufacturer of the Aloha POS system used by Chipotle, published a guide regarding best practices for maintaining a vulnerability management program regarding restaurants' POS systems.[35] Radiant Systems recommended that restaurants "install an antivirus application on all computers on the POS network." *Id.* Radiant Systems further recommended that restaurants "update virus definitions on a frequent, and regular basis. Update security patches for all installed software within one month of release." U.S. CERT also recommends using antivirus software.[36]

81. [redacted]

[35] *CISP Compliance Best Practices*, http://www.texaspos.com/Links/CISP%20Compliance.pdf.

[36] U.S. CERT, *Alert (TA14-002A), supra* n.21.

[redacted]

82. Furthermore, the Payment Card Data was unencrypted at the POS terminal, which would have prevented exfiltrated Payment Card Data from being publicly exposed.[37]

83. Payment Card Data for a purchase transaction must flow through multiple systems and parties in order to be processed. For most merchants, there are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen because it exists "in the clear":

- Pre-authorization – When the merchant has captured the Payment Card Data and it is being sent or is waiting to be sent to the acquirer/processor.
- Post-authorization – When Payment Card Data has been sent back to the merchant with the authorization response from the acquirer/processor, and it is placed into some form of storage in the merchant environment and used for analytics and other back-office processes.

84. First Data, the largest merchant acquirer, issuer processor, and independent network services provider in the world, recommends two highly effective technologies available to address these two specific points of vulnerability: encryption and tokenization.[38] "Encryption

[37] Kevin Lonergan, *Point of Sale malware takes a bite out of Wendy's fast food chain*, INFORMATIONAGE (June 10, 2016), http://www.information-age.com/technology/security/123461588/point-sale-malware-takes-bite-out-wendys-fast-food-chain.

[38] *See* First Data Market Insight, Avoiding a Data Breach: An Introduction to Encryption and Tokenization, https://www.firstdata.com/en_ie/insights/6203-Data-Breach-Market-Insight.html; *see also* Point of Sale Security: Retail Data Breaches At a Glance, DATACAP

mitigates security weaknesses that exist when [Payment Card Data] has been captured but not yet authorized. Tokenization addresses security vulnerabilities after a transaction has been authorized."[39] As First Data explains:

> In the process of tokenization, once the transaction is authorized the payment data is sent to a centralized and highly secure server where it is stored. At the same time, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The token number—which cannot be monetized by anyone but the merchant that owns the token—can be used in subsequent post-authorization business processes. . . . If token numbers are breached, they are meaningless to data thieves because they are simply random numbers. *Id*.

85. The National Restaurant Association has published certain information or best practices to protect restaurant networks from hacking. Specifically, the National Restaurant Association identified certain items within a restaurant's network that it should protect including that restaurants: "[e]nsure all credit card data is encrypted. If you have older POS equipment that sends raw credit card data to a back-office server, it may be time to upgrade. Modern, secure POS systems encrypt credit card data as soon as a card is swiped, and they immediately send that data to the payment processor without temporarily storing data. Double-check your POS system to make sure it complies with PCI standards."[40]

86. Had Chipotle employed certain best practices regarding encryption and tokenization of Payment Card Data at the POS terminal, it could have prevented the theft of Payment Card Data.

SYSTEMS, INC. (May 12, 2016), https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#.

[39] First Data Market Insight, *supra*.

[40] *6 measures to protect your network from hackers*, NAT'L REST. ASSOC., http://www.restaurant.org/Manage-My-Restaurant/Operations/Regulatory-back-office/4-measures-to-protect-your-network-from-hackers (last visited October 27, 2017).

6. Chipotle Failed to Install Software to Adequately Track and Monitor Its Network

87. Chipotle failed to adequately track access to its network and to monitor the network for unusual activity, particularly with respect to its POS terminals, which would have allowed Chipotle to detect and potentially prevent hackers from stealing Payment Card Data. One software vendor, Symantec, provides the following explanation regarding its endpoint protection software: "Symantec's network threat protection technology analyzes incoming data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are also included to protect against web-based attacks."[41]

88. Specifically, had Chipotle implemented proper endpoint detection and prevention systems, it would have been able to identify suspicious activity occurring within its network. Additionally, proper endpoint detection would have triggered warnings and alerted Chipotle to the transmission of Payment Card Data within its systems and should have alerted Chipotle to large volumes of data being removed, or exfiltrated, from its network.

89. Of course, warnings and alerts are only valuable to the extent the IT department reviews the logs of those warnings and alerts. [redacted]

[41] Data Sheet, Symantec Corporation, Symantec™ Endpoint Protection 12.1.6 (2015), https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-en.pdf (last visited October 27, 2017).

7. Chipotle Chose Not to Upgrade Its Payment Systems to Utilize EMV Technology

90. The payment card industry (MasterCard, Visa, Discover, and American Express) set a deadline of October 1, 2015 for businesses to transition their POS systems from magnetic stripe to EMV technology. Chipotle chose not to comply with that deadline.

91. EMV technology uses embedded computer chips, instead of magnetic stripes, to store Payment Card Data. Unlike magnetic stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used 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.

92. In 2015, Chipotle reported that it would not upgrade its terminals to EMV technology, claiming that it would slow down customer lines.[42] The IT Governance USA Blog reported that although no reason was given for not implementing EMV technology, "the large costs in overhauling the infrastructure in its 2,000-plus locations was almost certainly a factor, as is the fact that chip and PIN payments take longer than swiping cards."[43] The IT Governance USA Blog further reported that Absolute Software's Richard Henderson, stated that card swiping is incredibly lucrative to Chipotle and that the Company actively encourages customers to pay

---

[42] *See* Nicholas Upton, *Busing Chip-and-Pin Upgrade Myths*, FOODSERVICE NEWS (Sept. 2015), www.foodservicenews.net/The-FSN-Feed/September-2015/Busting-Chip-and-Pin-Upgrade-Myths/.

[43] Luke Irwin, *Chipotle warns customers of a possible payment card breach*, IT GOVERNANCE (May 8, 2017), https://www.itgovernanceusa.com/blog/chipotle-warns-customers-of-a-possible-payment-card-breach/.

with cards "to speed up transactions and keep their long lines moving fast." *Id.* According to Henderson, "it's no wonder they were targeted by cyber criminals." *Id.*

93. Chipotle, thus, knowingly left Payment Card Data vulnerable to theft. If Chipotle had employed EMV technology, it could have prevented the Data Breach. [redacted].

94. Despite the fact that Defendant was put on notice of the very real possibility of Payment Card Data theft associated with its security practices, and despite the fact that Defendant knew or, at the very least, should have known about the elementary infirmities associated with Chipotle's POS and security systems, it still chose not to make necessary upgrades to its systems and security practices and protocols.

D. In Breaching Its Duty to Not Create Risk of Harm to Others, Chipotle Chose Not to Follow Industry Standards of Care

95. Chipotle's adherence to reasonable industry standards of care would have either prevented or timely detected this Data Breach. In addition to the best practices discussed above, the payment card industry and federal agencies have issued recommended standards of care regarding adequate data security measures.

96. Given the extensive network of financial institutions involved in payment card transactions and the sheer volume of daily transactions using credit and debit cards, it is unsurprising that financial institutions and credit card processing companies have issued rules

and standards governing the basic measures that merchants must take to ensure consumers' valuable data is protected.

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

98. The 12 requirements of the PCI DSS are:

Build and Maintain a Secure Network

1) Install and maintain a firewall configuration to protect cardholder data

2) Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3) Protect stored cardholder data

4) Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5) Use and regularly update antivirus 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) Assign a unique ID to each person with computer access

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 employees and contractors.[44]

99. Furthermore, PCI DSS 3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

100. 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 its daily collection and transmission of tens of thousands of sets of Payment Card Data. [redacted]

101. Similarly, U.S. CERT, part of the Department of Homeland Security, issued Alert TA14-002A on January 2, 2014, titled "Malware Targeting Point of Sale Systems."[45] The document discusses hardware and software attacks against POS systems and includes specific best practices recommended to protect POS systems. *Id*. *See also* John H. Sawyer, *Tech Insight Defending Point-Of-Sale Systems*, InformationWeek (Jan. 24, 2014), https://www.darkreading.com/attacks-breaches/tech-insight-defending-point-of-sale-systems/d/d-id/1141214.

---

[44] PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2*, at 9 (May 2016), https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security.

[45] U.S. CERT, *Alert (TA14-002A)*, *supra* n.21.

102. The Cybersecurity Framework developed by NIST, the federal agency that works with industry to develop and apply technology, measurements, and standards, also provides businesses with guidance on best practices. The Cybersecurity Framework cites numerous industry standards available to guide businesses in adopting best practices, including the Information Systems Audit and Control Association's ("ISACA") Control Objectives for Information and Related Technology ("COBIT"), the Council on CyberSecurity's Top 20 Critical Security Controls, the International Society of Automation's Standards (such as ANSI/ISA-62443-2-1 (99.02.01)-2009 and ANSI/ISA-62443-3-3 (99.03.03)-2013), and the International Organization for Standardization's ISO/IEC 27001:2013.[46]

103. According to the *ISACA Journal*, the Enterprise Strategy Group found that 72 percent of North American organizations with 1,000 or more employees have implemented one or more formal IT best-practice control and process models and standards such as COBIT and ISO/IEC 27001 and 27002.[47]

104. COBIT 5 provides management practices and monitoring processes to adequately protect organizations from internal and external data threats. *Id.* Specifically, COBIT 5 Management Practices recommend that organizations implement the following:

- APO 13.01 – Establish and maintain an information security management system.
- DSS 05.01 – Protect against malware.
- DSS 05.02 – Manage network and connectivity security.

---

[46] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/cyberframework.

[47] Mathew Nicho, Ph.D., CEH, SAP-SA, RWSP, and Hussein Fakhry, Ph.D., *Using COBIT 5 for Data Breach Prevention*, ISACA Journal (2013), https://www.isaca.org/Journal/archives/2013/Volume-5/Pages/Using-COBIT-5-for-Data-Breach-Prevention.aspx#2 (last accessed October 29, 2017).

- DSS 05.03 – Manage endpoint security.
- DSS 05.04 – Manage user identity and logical access.
- DSS 05.05 – Manage physical access of IT assets.

Id.

105. The ISO and the International Electrotechnical Commission ("IEC") have likewise developed standards and models for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security management systems. ISO/IEC 27001 sets forth a check list and control objectives for information security policies for organizations to protect their information systems and networks.[48] Specifically, the control objectives include:

> **A.5.1 Information Security Policy:** Objective: to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
>
> **A.6.1.1 Management Commitment to Information Security:** Control – Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
>
> **A.10.3 System planning and acceptance:** Objective: To minimize the risk of systems failures. **A.10.3.2 System acceptance:** Control – Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
>
> **A.10.4 Protection against malicious and mobile code: O**bjective: To protect the integrity of software and information. **A.10.4.1 Controls against malicious code:** Control – Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
>
> **A.10.6 Network security management:** Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure. **A.10.6.1**

---

[48] ISO/IEC 27001 (2005), *available at* http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf.

> **Network controls:** Control – Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
>
> **A.10.10 Monitoring:** Objective: To detect unauthorized information processing activities. **A.10.10.1 Audit logging:** Control – Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
>
> **A.11.4 Network access control:** Objective: To prevent unauthorized access to networked services. **A.11.4.1 Policy on use of network services:** Control – Users shall only be provided with access to the services that they have been specifically authorized to use.
>
> **A.11.4.7 Network routing control**: Control – Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
>
> **A.12.4 Security of system files:** Objective: To ensure the security of system files. **A.12.4.1 Control of operational software:** Control – There shall be procedures in place to control the installation of software on operational systems.
>
> **A.13.1 Reporting information security events and weaknesses:** Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. **A.13.1.1 Reporting information security events:** Control – Information security events shall be reported through appropriate management channels as quickly as possible.

Id. at 13-26.

106. Similarly, ISO/IEC 27002 provides additional, specific best practice recommendations on information security management systems.[49] ISO 27002 states that in order to properly protect against malicious and mobile code and to protect the integrity of software and the organization's information, the following guidance should be observed:

[49] ISO/IEC 27002 (2005), *available at* http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf (last accessed October 29, 2017).

> Implementation guidance: Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

Id.

107. Visa also frequently provides merchants with best practices tips. For example, in May 2009, Visa issued an updated Data Security Alert instructing merchants to secure their POS environments by, among other things, implementing egress and ingress filtering, network segmentation, firewalls, file integrity monitoring, updated antivirus software programs, and protocols for routine monitoring of computer systems.[50]

108. Because Chipotle stores accepted payment cards containing sensitive financial and personal information, Defendant knew that financial institutions, such as Plaintiffs and the Class, were entitled to, and did, rely on Defendant to keep that sensitive information secure from would-be data thieves in accordance with at least the PCI DSS requirements. Chipotle did not even meet this minimum standard of care, much less even attempt to comply with other well-known industry best practices.

E. Federal and State Statutes Create a Statutory Duty to Not Engage in Unfair Practices

1. The FTC Act and Similar State Statutes

109. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, such as Payment Card Data, constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

---

[50] Data Security Alert – *Targeted Hospitality Sector Vulnerabilities*, *supra* n.17.

110. 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 networks' 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.

111. The FTC also has 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.[51]

112. The FTC also has issued numerous 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.

113. In addition, individual states have enacted statutes based upon the FTC Act that also create a statutory duty to not engage in unfair business practices. Specifically, the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*., Florida's Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*., Maine Unfair Trade

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

Practices Act, 5 M.R.S.A §§ 205-A, *et seq*., Massachusetts Consumer Protection Act, Mass. Gen. Laws Ch. 93A, *et seq*., New Hampshire Consumer Protection Act, N.H. Stat. §§ 358-A:1, *et seq*., and Vermont Consumer Fraud Act, 9 V.S.A §§ 2451, *et seq*., prohibit unfair trade practices. Each statute is interpreted consistently with Section 5 of the FTC Act, with consideration given to the interpretation and construction given to Section 5 by the FTC and federal courts.

2. State Statutes Provide Guidance Regarding the Standard of Care Required to Protect Data

114. Several state laws also provide guidance regarding the standard of care required to protect personal and financial information contained in the Payment Card Data that is acquired by and entrusted to businesses like Chipotle. *See* Ark. Code § 4-110-104(b);, Cal. Civ. Code §§ 1798.81, 1798.81.5; Fla. Stat. § 501.171(2); and Mass. Gen. Laws Ch. 93H § 2(a). These statutes require businesses, like Chipotle, to implement and maintain reasonable security procedures and practices to protect the personal and financial information, which is contained in Payment Card Data, to prevent unauthorized access, destruction, use, modification, or disclosure of the information.

115. The FTC Act and its state law counterparts at a minimum provide a reasonable standard of care, if not a statutory duty, with which Chipotle did not even attempt to comply.

F. The Property Damage and Financial Losses that Financial Institutions Have Suffered, and Will Continue to Suffer, Were Foreseeable

116. Processing a payment card transaction involves four major steps:

Authorization – when a customer presents a card to make a purchase, Chipotle requests authorization of the transaction from the card's issuer using the Payment Card Data from the card presented;

Clearance – if the issuer authorizes the transaction, Chipotle completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;

Settlement – the acquiring bank pays Chipotle for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and

Post-Settlement – the issuer posts the charge to the customer's credit or debit account.

117. Payment Card Data is central to the payment card transaction process. For financial institutions, like Plaintiffs, Payment Card Data is an asset that has significant value. Payment Card Data is owned by the financial institution, not the cardholder; the cardholder is merely an authorized user. Payment Card Data is kept by financial institutions in the form of computer data,[52] stored as records in a secured database on a financial institution's computer system. [53] In addition, the Payment Card Data is encoded on the magnetic stripe of the payment card. Payment Card Data is a financial institution's means of authenticating the cardholder and authorizing a payment card transaction.

118. To authorize a transaction, the issuing financial institution receives, from the merchant, the Payment Card Data that is encoded on the payment card being used by the consumer. The issuing financial institution's computer uses the Payment Card Data, received

---

[52] Computer data is "any representation of knowledge, facts, concepts, instruction, or other information computed, classified, processed, transmitted, received, retrieved, originated, stored, manifested, measured, detected, recorded, reproduced, handled, or utilized by a computer, computer network, computer program, or computer software, and may be in any medium[.]" N.H. Rev. Stat. § 638:16, V.

[53] "Each row of a database comprises a single record made up of multiple distinct pieces of information, and each column of the database table represents an attribute of that record." A SANS Inst. Whitepaper- November 2007, REGULATIONS AND STANDARDS: WHERE ENCRYPTION APPLIES. For example, a record of protected stored Payment Card Data for the financial institutions will include, but not be limited to the following sensitive information: the cardholder name, address, primary account numbers, and associated financial information such as expiration date, daily limits, and service codes.

from the merchant, to locate the computer data on the financial institution's computer for the payment card's specific record. The financial institution then uses the payment card's specific record stored on its computer to authorize the transaction. The transaction authorization process relies on the Payment Card Data being known only to the parties to the payment card transaction.

119. When Payment Card Data (that is stored on financial institutions' computer systems and used to securely authorize financial transactions) is compromised, the computer database record that contains the compromised Payment Card Data is no longer usable to securely authorize transactions. Due to the disclosure of the Payment Card Data to third parties, the computer data for the specific payment card becomes susceptible to fraud, and therefore, loses its integrity.

120. "Integrity" is a fundamental attribute of computer data. *See*, *e.g.*, 44 U.S.C. § 3542(b)(1)(A) (defining integrity as an attribute of the federal government's information security policy). "Integrity generally refers to maintaining computer data in a protected state, unaltered by improper, unauthorized or subversive conduct or acts contrary to what the system owner or privilege grantor intended. Integrity concerns computer data stored, processed, or in transit. In the context of databases, integrity also regards metadata and the functions involved."[54]

121. When a data breach occurs, the computer database record that contains the compromised Payment Card Data is damaged and no longer usable to authorize transactions. In other words, the financial institution can no longer count on the person using the information to be the cardholder and cannot rely on its computer data to securely authorize transactions. The Payment Card Data therefore effectively is rendered commercially worthless.

---

[54] Ioana & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. PITT. J. TECH. L. & POL'Y 158 (2014).

122. Thus, when Payment Card Data has lost its integrity, the financial institution must issue a replacement payment card with new Payment Card Data to prevent fraud. As a result, the computer data (database record) that contains the compromised Payment Card Data must be replaced with new computer data (database record) that matches the newly issued Payment Card Data.

123. These actions are not optional for the financial institutions. For example, the Gramm-Leach-Bliley Act ("GLBA") mandates that financial institutions protect the security and confidentiality of consumer nonpublic personal information at all times. *See* 15 U.S.C.A. §§ 6801-6809.

124. Federal and state laws recognize that computer data, like Payment Card Data,[55] is property[56] that suffers "damage" when it has lost its integrity and been rendered unusable. *See*,

---

[55] State laws recognize Payment Card Data as computer data. *See*, *e.g.*, Ark. Code Ann. § 5-41-102(7) (defining computerized "data" as "any representation of information, knowledge, a fact, concept, or an instruction that is being prepared or has been prepared and is intended to be processed or stored, is being processed or stored, or has been processed or stored in a computer, computer network, or computer system"); Ark. Code Ann. § 5-41-201(4) (defining "data" as "a representation of any form of information, knowledge, a fact, concept, or an instruction that is being prepared or has been formally prepared and is intended to be processed, is being processed, or has been processed in a system or network"); N.H. Rev. Stat. § 638:16, IV (defining "computer data" as "any representation of knowledge, facts, concepts, instruction, or other information computed, classified, processed, transmitted, received, retrieved, originated, stored, manifested, measured, detected, recorded, reproduced, handled, or utilized by a computer, computer network, computer program, or computer software, and may be in any medium, including, but not limited to, computer print-outs, microfilm, microfiche, magnetic storage media, optical storage media, punch paper tape, or punch cards, or it may be stored internally in read-only memory or random access memory of a computer or any other peripheral device").

[56] State laws recognize that "property" includes computerized data. *See*, *e.g.*, Ark. Code Ann. § 5-41-102(10) ("'Property' includes, but is not limited to, a financial instrument, data, computer program, document associated with a computer or computer program, or a copy of a financial instrument, data, computer program, or document associated with a computer or computer program, whether tangible or intangible, including both human and computer readable

e.g., 18 U.S.C. §§ 1030(e)(8), (11) (defining "damage" as "any impairment to the integrity or availability of data, a program, a system, or information;" and, "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service"); C.R.S.A. § 18-5.5-101(6.3) ("'Damage' includes, but is not limited to, any impairment to the integrity of availability of information, data, computer program, computer software, or services on or via a computer, computer network, or computer system or part thereof."); *see also* Ark. Code Ann. §§ 5-41-101 (recognizing that the opportunities for "the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great" and that "[l]osses from [such incidents] are potentially astronomical"); Ark. Code Ann. § 5-41-106 (providing a private right of action to recover for damage to computer data); Ark. Code Ann. § 5-41-202 (recognizing acts that harm computer data as unlawful); N.H. Rev. Stat. § 638:17, IV(b) (recognizing damage to computer data as a crime).

125. In short, Payment Card Data kept as computer data is Plaintiffs' and the Class's means of authenticating the cardholder and authorizing a transaction. When the Payment Card Data reflected in the computer data was compromised in the Data Breach, the computer data was

---

data, and data while in transit"); Ark. Code Ann. § 5-41-201(10) (defining "property" as "anything of value and includes a financial instrument, information, electronically produced data, program, and any other tangible or intangible item of value"); N.H. Rev. Stat. § 638:16, XVI (defining "property" to include "computer data . . . regardless of whether [it is]: (1) Tangible or intangible; (2) In a format readable by humans or by a computer; (3) In transit between computers or within a computer network or between any devices which comprise a computer; or (4) Located on any paper or in any device on which it is stored by a computer or by a human"); C.R.S.A. § 18-5.5-101(8) ("'Property' includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value").

damaged because it lost its integrity and Plaintiffs and the Class no longer could rely on it to authorize transactions. In other words, Plaintiffs and the Class no longer can count on the person using the information to be the cardholder and cannot rely on its computer data to securely authorize transactions. Therefore, Chipotle, by implementing inadequate data security measures, caused Plaintiffs and the Class to suffer property damage.

126. The property damage suffered by Plaintiffs and the Class was foreseeable to Defendant. Defendant knew that implementing data security measures that were inadequate to protect Payment Card Data would cause harm to the card-issuing institutions, such as Plaintiffs and the Class, because the issuers are financially responsible for fraudulent card activity, *see* 12 C.F.R. § 1005.6, 12 C.F.R. § 1026.12, and must incur significant costs to prevent additional fraud. Indeed, Defendant's public statement to customers after the Data Breach, when it stated "[i]f anyone sees an unauthorized charge, they should immediately notify the bank that issued the card,"[57] plainly indicates that Defendant believes that card-issuing institutions, like Plaintiffs and the Class, should be responsible for fraudulent charges on cardholder accounts resulting from the Data Breach.

127. As the direct and proximate result of Chipotle's conduct, Plaintiffs have suffered and will continue to suffer irreparable injury and significant property damage and financial losses. Specifically, Plaintiffs and other financial institutions have been forced to: (a) replace the computer data rendered useless by the Data Breach; (b) cancel or reissue any credit and debit cards affected by the Data Breach; (c) close any deposit, transaction, checking, or other accounts affected by the Data Breach, including, but not limited to, stopping payments or blocking

[57] *Notice of Data Security Incident*, CHIPOTLE MEXICAN GRILL, *supra* n.11.

transactions with respect to the accounts; (d) refund any cardholder for any unauthorized transaction relating to the Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

128. Moreover, Plaintiffs' and the Class's business is reliant on their reputation and customer relationships and their ability to maintain and grow their customer base in a competitive market. By engaging and continuing to engage in the conduct and activities described herein, Chipotle inevitably will be subject to a data breach again.

G. Payment Card Data Is Protectable Trade Secret Information that Chipotle Has Misappropriated

129. Payment Card Data is protectable trade secret information under the DTSA, 18 U.S.C. §§ 1831, *et seq*. The definition of "trade secrets" under § 1839(3) of the DTSA, is broad and generally covers "all forms and types of" protected information, regardless of how it is stored.

130. Financial institutions, like Plaintiffs and the Class, devote substantial effort, resources, time and investment to develop, create, use and protect the confidence of Payment Card Data. The protected Payment Card Data resides on the financial institutions' secure servers, with limited access and significant security protections.

131. Financial institutions, including Plaintiffs, take reasonable steps to protect the secrecy of Payment Card Data as part of their ongoing standard operating procedures to maintain the confidential nature of this information.

132. Financial institutions operate their business in interstate and foreign commerce, in that their payment card processing activities constitute the use of Payment Card Data in interstate and foreign commerce.

133. As statutorily required,[58] financial institutions have numerous safeguards in place to maintain the confidentiality of Payment Card Data and to protect against its unlawful use or disclosure throughout the payment card process. There also are significant limits on a financial institution's disclosure of Payment Card Data to third parties. For example, a financial institution must not disclose an account number or similar form of access number or access code for a payment card, to any nonaffiliated third party (other than a consumer reporting agency) for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. *See* 15 U.S.C.A. §§ 6801-6809.

134. As part of the measures to protect confidentiality and prevent unauthorized disclosure, payment cards are issued to consumers in an "inactive" status and must be "activated" by the financial institutions' customer prior to use. The payment card can only be activated in the manner the financial institutions specify. Payment card activation steps include confirmation of consumer identity and verification of the payment card via telephone call or online. The activation requirement is a security measure financial institutions use to ensure that the rightful customer actually received the card. The activation measures also serve to protect the secrecy of Payment Card Data and to ensure the confidential information contained on the

[58] *See*, *e.g.*, Fair Credit Reporting Act ("FCRA"), 15 U.S.C.A. §§ 1681, *et seq.*; Truth in Lending Act ("TILA"), 15 U.S.C.A. §§ 1601, *et seq.* and its implementing Regulation Z (12 C.F.R. Part 226); Equal Credit Opportunity Act, 15 U.S.C.A. §§ 1691, *et seq.* and its implementing Regulation B (12 C.F.R. Part 202); and GLBA, 15 U.S.C.A. §§ 6801, *et seq.*

payment card does not end up disclosed to an unintended third party. Only after a payment card is activated, can the consumer use it to make purchases.

135. In addition, the consumer must take steps to maintain the secrecy of the financial institutions' Payment Card Data. The FTC recommends that consumers keep payment cards in a safe place and use care in disclosure of the Payment Card Data.[59] Moreover, the consumers must notify the financial institution if the card is lost or stolen. *Id*.

136. Regarding usage of a payment card, Payment Card Data from the card is obtained from the magnetic stripe and verified at the time of purchase. It is absolutely critical that the Payment Card Data stays only between the parties to the transaction (the consumer and its issuing bank and the merchant and its acquiring bank). The importance of allowing access only to those parties necessary is evidenced by a myriad of security rules and regulations, such as PCI DSS, discussed above, and the Fair and Accurate Credit Transactions Act ("FACTA"), which prohibits a merchant from printing more than the last five digits of the payment card number or the expiration date on a receipt.

137. Financial institutions derive independent economic value from Payment Card Data not being generally known or readily ascertainable through proper means. Indeed, once Payment Card Data becomes known to unauthorized third parties, it is rendered useless for its intended purpose and must be replaced by the financial institutions.

138. As outlined above, Chipotle's business operations and payment systems are governed by PCI DSS, which gives rise to a duty to protect and maintain the secrecy of Plaintiffs' and the Class's Payment Card Data. Chipotle knew that Payment Card Data was

[59] How to Protect Your Cards and Account Information: For Credit and ATM or Debit Cards, https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

highly sensitive, protected information and still failed to reasonably maintain the requisite secrecy of Plaintiffs' and the Class's Payment Card Data.

139. Chipotle misappropriated Plaintiffs' and the Class's Payment Card Data by its unauthorized disclosure. Under the DTSA, the term "misappropriation" is defined broadly and includes improper use or disclosure. Chipotle misappropriated financial institutions' confidential, proprietary, and trade secret information through its disclosure of Payment Card Data, as described herein, without the express or implied consent of Plaintiffs and the Class, where Chipotle at the time of disclosure knew or had reason to know that it had acquired Payment Card Data under circumstances giving rise to a duty to maintain the secrecy of the Payment Card Data. *See* 18 U.S.C. § 1839(5)(B)(ii)(II).

CLASS ACTION ALLEGATIONS

140. Plaintiffs bring Counts Three and Eleven below individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23. The proposed Class is defined as:

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

141. Plaintiffs also bring Counts One, Two, Four, Five, Six, Seven, Eight, Nine and Ten below individually and on behalf of those defined below within the identified states pursuant to Fed. R. Civ. P. 23. Each proposed statewide Class is defined as:

> All Financial Institutions − including, but not limited to, banks and credit unions – that either: (a) are located in Arkansas, California, Florida, Maine, Massachusetts, New Hampshire, Virginia, Vermont, and Wisconsin that issue payment cards, including credit and debit cards, or perform, facilitate, or support

> card-issuing services, whose customers made purchases from Chipotle stores from March 1, 2017 to the present, or (b) have customers located in Arkansas, California, Florida, Maine, Massachusetts, New Hampshire, Virginia, Vermont, and Wisconsin that were issued payment cards used at Chipotle stores from March 1, 2017 to the present (the "Class").

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

143. **Numerosity**: All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of each Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believe that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiffs. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

144. **Commonality and Predominance**: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. whether Chipotle engaged in the misconduct alleged;

b. whether Chipotle implemented data security measures that were inadequate to detect and potentially prevent the Data Breach and protect Payment Card Data;

c. whether Chipotle owed a duty to Plaintiffs and Class members and whether Chipotle violated that duty;

d. whether Chipotle engaged in unfair or unlawful acts and practices in violation of state consumer protection statutes;

e. whether Plaintiffs' and the Class's Payment Card Data constitutes protectable trade secrets that Chipotle misappropriated;

f. whether Plaintiffs and Class members were injured and suffered damages or other ascertainable loss as a result of Chipotle's conduct; and

g. whether Plaintiffs and Class members are entitled to relief and the measure of such relief.

145. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Each Plaintiff is a member of the Class, having issued payment cards that were compromised in the Data Breach. Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendant's conduct and Plaintiffs and each Class are asserting claims based on the same legal theories.

146. **Adequacy**: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Each Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Each Plaintiff is committed to pursuing this matter for the Class with the Class's collective best

interests in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

147. **Superiority**: The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Chipotle, so it would be impracticable for members of the Class to individually seek redress for Chipotle's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

148. **Injunctive and Declaratory Relief**: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to each Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

COUNT ONE

Negligence

149. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

150. Defendant owed – and continues to owe – a duty to Plaintiffs and the Class to use and exercise reasonable care in obtaining and processing Plaintiffs' and the Class's Payment Card Data. This duty arises from the common law and statute and is independent of any duty Chipotle owed as a result of its contractual obligations.

151. Chipotle has an independent common law duty of reasonable care to prevent the foreseeable risk of harm to others, including Plaintiffs and the Class. It was entirely foreseeable to Chipotle that injury would result from the use of inadequate and unreasonable data security measures to protect Payment Card Data. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Plaintiffs' and the Class's Payment Card Data; thieves would use Payment Card Data to make large numbers of fraudulent transactions; and, as a result, Plaintiffs and the Class would be required to replace the computer data rendered useless by the Data Breach, cancel and reissue the compromised payment cards, and reimburse their customers for any unauthorized transactions relating to the Data Breach.

152. Plaintiffs and the Class thus seek to recover for Chipotle's breach of an independent duty to not create unreasonable risk with regard to Plaintiffs' and the Class' Payment Card Data. Chipotle had a duty to employ reasonable data security measures because inadequate measures foreseeably create an unreasonable risk that Plaintiffs' and the Class' Payment Card Data would be compromised, with substantial property damage and financial loss

resulting. In failing to maintain reasonable security measures, Chipotle created the risk of the harm that occurred and Plaintiffs and the Class were the foreseeable victims of that harm.

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

154. Defendant knew or should have known that its implementation of inadequate and unreasonable data security measures to protect its POS terminals against obvious risks would result in harm to Plaintiffs and the Class.

155. By accepting payment cards, Chipotle also voluntarily assumed the duty to use reasonable security measures. When a company, such as Chipotle, through the ordinary course of its business (and for its own economic benefit) receives, gathers, and/or stores Payment Card Data, it has undertaken to render services necessary for the protection of that property, and therefore has an affirmative duty to take reasonable efforts to provide security for that property.

156. A duty to use reasonable security measures also arose as a result of the special relationship that existed between Chipotle and Plaintiffs and the Class. The special relationship arose because financial institutions entrusted Chipotle with Payment Card Data from payment cards they issued. Only Chipotle was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

157. Moreover, Section 5 of the FTC Act imposes a statutory duty on merchants to not engage in unfair business practices, which the FTC repeatedly has determined includes the duty to use reasonable data security measures. In addition, individual states have enacted statutes

based on the FTC Act, as alleged herein, that also create a statutory duty to not engage in unfair business practices.

158. Defendant breached its common law and statutory duties when it knowingly: (a) ignored well-known data security risks, thereby intentionally allowing data security deficiencies to persist; (b) disregarded warnings that its Aloha POS system was incompatible with the antivirus software, which frequently resulted in system crashes; (c) refused to upgrade the POS system when the manufacturer ceased providing security or technical updates for the POS operating system, which made the POS system highly vulnerable to attack; (d) lacked adequate firewall protection and proper network segmentation, which would have prevented hackers from accessing Payment Card Data; (e) refused to implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its POS and other systems that accessed Payment Card Data and otherwise would have protected Payment Card Data; (f) failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of the hacker and prevented Payment Card Data from being stolen; and (g) chose not to implement EMV technology for use with its POS systems, which would have provided complete protection for Payment Card Data.

159. [redacted]

[redacted].

160. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class have suffered and continue to suffer substantial property damage and financial losses as detailed herein.

COUNT TWO

Negligence *Per Se*

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

162. 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.

163. Chipotle violated § 5 of the FTC Act (and similar state statutes) by implementing unreasonable data security measures that were inadequate to protect Payment Card Data. 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.

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

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

166. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

167. As a direct and proximate result of Chipotle's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, substantial property damage and financial losses as detailed herein.

COUNT THREE

Misappropriation of Trade Secrets (18 U.S.C. §§ 1831, *et seq.*)

168. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

169. Plaintiffs' and the Class's customers utilize the financial institutions' payment cards to engage in interstate and foreign commerce.

170. Plaintiffs' and the Class's Payment Card Data qualifies as "trade secrets" under the DTSA, which covers "all forms and types of" protected information, regardless of how it is stored. 18 U.S.C. § 1839(3).

171. Plaintiffs and the Class obtain economic value from Payment Card Data not being generally known or readily ascertainable through proper means.

172. Plaintiffs and the Class have taken reasonable steps and precautions to safeguard Payment Card Data and to limit and restrict others from knowing, readily ascertaining or using Payment Card Data, as described herein.

173. Chipotle knew it had a duty to maintain the secrecy of Plaintiffs' and the Class's trade –secret-protected Payment Card Data due, in part, to PCI DSS Standards.

174. Chipotle has misappropriated through unauthorized disclosure Plaintiffs' and the Class's confidential, proprietary, and trade-secret-protected Payment Card Data.

175. As a result of Chipotle's improper misappropriation through unauthorized disclosure of Plaintiffs' and the Class's trade secrets, it has violated the DTSA.

176. Plaintiffs' and the Class's business is reliant on their reputation and customer relationships and their ability to maintain and grow their customer base in a competitive market. As the direct and proximate result of Chipotle's conduct, Plaintiffs have suffered and, if Chipotle is not enjoined, will continue to suffer irreparable injury and significant damages in an amount to be proven at trial.

177. By engaging and continuing to engage in the conduct and activities described herein, Chipotle has disclosed and will inevitably disclose again protected Payment Card Data of Plaintiffs and the Class. If Chipotle's conduct is not remedied and if Defendant is not enjoined,

Defendant will continue to misappropriate through unauthorized disclosure Plaintiffs' and the Class's Payment Card Data to their detriment.

178. Chipotle's actual and threatened misappropriation of Payment Card Data is causing Plaintiffs and the Class to suffer irreparable harm, including but not limited to loss of customers, loss of reputation and customer goodwill, and loss of its investment in its trade secrets. This harm cannot be adequately remedied at law and requires permanent injunctive relief.

179. Because Plaintiffs' and the Class's damages cannot be adequately compensated through remedies at law alone, Plaintiffs and the Class seek permanent injunctive relief to recover and protect their Payment Card Data and other legitimate business interests. Plaintiffs and the Class will continue to suffer irreparable harm absent injunctive relief from this Court.

180. Chipotle's actions in misappropriating Plaintiffs' and the Class's Payment Card Data were willful, wanton and malicious, and were taken with reckless disregard for the rights of Plaintiffs and the Class.

181. Plaintiffs and the Class are entitled to full compensatory, exemplary, and consequential damages, as well as full attorneys' fees, costs and expenses.

COUNT FOUR

Violation of the Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-101, *et seq.*

(On Behalf of Plaintiff Alcoa and the Arkansas Class)

182. Plaintiff Alcoa incorporates and realleges each and every allegation contained above as if fully set forth herein.

183. Plaintiff Alcoa brings this claim on behalf of itself and the Arkansas Class pursuant to the Arkansas Deceptive Trade Practices Act ("ADTPA"), Ark. Code Ann. §§4-88-101, *et seq*.

184. Plaintiff Alcoa and the Arkansas Class are "persons" within the meaning of the ADTPA. Ark. Code Ann. § 4-88-102(5).

185. Plaintiff Alcoa has suffered an "actual financial loss" as it has lost "an ascertainable amount of money" as a result of Chipotle's unconscionable acts and practices. Ark. Code Ann. § 4-88-102(9).

186. The ADTPA prohibits unconscionable acts or practices in business, commerce, or trade. Ark. Code Ann. §§4-88-107(10).

187. Chipotle engaged in unconscionable acts and practices in business, commerce, or trade under ADTPA by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unconscionable practices occurred repeatedly in connection with Chipotle's trade or business.

188. Chipotle's affirmative acts in adopting and maintaining inadequate security measures are unconscionable within the meaning of ADTPA because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition.

189. Chipotle's failure also was unconscionable within the meaning of ADTPA because its conduct undermined Arkansas public policy that businesses protect personal and financial information, as reflected in Ark. Code Ann. § 4-110-102.

190. Plaintiff Alcoa and the Arkansas Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

191. Chipotle has engaged in unconscionable consumer-oriented acts or practices and has injured Plaintiff Alcoa and the Arkansas Class by such acts and practices. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Alcoa and the Arkansas Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Alcoa and the Arkansas Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

192. Plaintiff Alcoa and the Arkansas Class have members located in Arkansas who used Plaintiff's and the Class's payment cards to purchase food for personal consumption from Chipotle and whose payment cards were impacted by the Data Breach. For these Arkansas-based cardholders, Plaintiff Alcoa and the Arkansas Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Through these acts, Plaintiff Alcoa and the Arkansas Class suffered concrete and substantial injuries in Arkansas.

193. Chipotle willfully engaged in the unconscionable acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the ADTPA.

194. As a direct and proximate result of Chipotle's unconscionable practices and violation of ADTPA, Plaintiff Alcoa and the Arkansas Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT FIVE

Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Based on "Unfair" and/or "Unlawful" Acts and Practices

(On Behalf of Plaintiff Bellwether and the California Class)

195. Plaintiff Bellwether incorporates and realleges each and every allegation contained above as if fully set forth herein.

196. Plaintiff Bellwether brings this claim on behalf of itself and the California Class pursuant to the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.

197. Plaintiff Bellwether and Chipotle are "persons" within the meaning of Cal. Bus. & Prof. Code § 17201.

198. The UCL prohibits unfair competition, which includes an "unlawful, unfair or fraudulent" act or practice. Cal. Bus. & Prof. Code § 17200.

199. Under the UCL, any business act or practice that is unethical, oppressive, unscrupulous, and/or substantially injurious to consumers, or that violates a legislatively declared policy, constitutes an unfair business act or practice.

200. The violation of any law constitutes an unlawful business practice under the UCL.

201. Chipotle engaged in unfair and unlawful business practices prohibited by the UCL by unreasonably adopting and maintaining data security measures that were inadequate to protect

Payment Card Data and prevent the Data Breach. These unfair and unlawful practices occurred repeatedly in connection with Chipotle's trade or business.

202. Chipotle's affirmative acts in adopting and maintaining inadequate data security measures are unfair within the meaning of the UCL, because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition.

203. Chipotle's implementation of inadequate data security measures also was unfair within the meaning of the UCL, because its conduct undermined California public policy that businesses protect personal and financial information as reflected in Article I, Section 1 of the California Constitution (enacted because of private sector data processing activity and stating that all people have an inalienable right to privacy) and in statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22578 (explaining that the Legislature's intent was to have a uniform policy statewide regarding privacy policies on the Internet); the Information Practices Act, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a)(1) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); and the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits unfair trade practices.

204. Chipotle's violations of the California Customer Records Act, Cal. Civ. Code § 1798.81.5(b) (the "California Customer Records Act"), moreover, constitute unlawful acts or practices under the UCL. The "California Customer Records Act requires a "business that owns,

licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Chipotle failed to implement and maintain such reasonable security procedures and practices before and at the time of the Data Breach. As a result, Chipotle violated the California Customer Records Act, Cal. Civ. Code § 1798.81.5(b).

205. Chipotle's violations of the FTC Act, 15 U.S.C. § 45(a)(1), as alleged herein, also constitute unlawful acts or practices under the UCL.

206. Plaintiff Bellwether and the California Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

207. Chipotle's conduct harmed competition. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure Payment Card Data was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Bellwether and the California Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Bellwether and the California Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

208. Plaintiff Bellwether and the California Class have members located in California whose payment cards were impacted by the Data Breach. For these California-based cardholders, Plaintiff Bellwether and the California Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff Bellwether and the California Class suffered an injury in California.

209. Chipotle willfully engaged in the unfair and unlawful acts and practices described above and knew or should have known that those acts and practices were unfair and unlawful in violation of the UCL.

210. As a direct and proximate result of Chipotle's unfair and unlawful practices and violation of UCL, Plaintiff Bellwether and the California Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT SIX

Violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*

(On Behalf of Plaintiff Bellwether and the Florida Class)

211. Plaintiff Bellwether incorporates and realleges each and every allegation contained above as if fully set forth herein.

212. Plaintiff Bellwether brings this claim on behalf of itself and the Florida Class pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et seq*.

213. Plaintiff Bellwether and members of the Florida Class are "consumers" within the meaning of Fla. Stat. § 501.203(7).

214. Defendant is engaged in "trade or commerce" within the meaning of Fla. Stat. § 501.203(8).

215. FDUTPA prohibits unfair acts or practices in the conduct of trade or commerce. An "unfair practice" within the meaning of FDUTPA is one that offends established public policy or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers. Violations of "[t]he standards of unfairness and deception set forth and interpreted by the Federal Trade Commission" also violate FDUTPA. *See* Fla. Stat. Ann. § 501.203(3)(b).

216. Chipotle engaged in unfair business practices prohibited by FDUTPA by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Chipotle's trade or business.

217. Chipotle's affirmative acts in adopting and maintaining inadequate security measures is unfair within the meaning of FDUTPA because it constituted an immoral, unethical, oppressive, and unscrupulous activity; caused substantial injury to consumers and businesses; and provided no benefit to consumers or competition.

218. Chipotle's failure also was unfair within the meaning of FDUTPA because its conduct undermined Florida public policy that businesses protect personal and financial information as reflected in Fla. Stat. §§ 501.171(2), (9)(a).

219. Plaintiff Bellwether and the Florida Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

220. Chipotle's conduct harmed competition. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Bellwether and the Florida Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Bellwether and the Florida Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

221. Plaintiff Bellwether and the Florida Class have members located in Florida whose payment cards were impacted by the Data Breach. For these Florida-based cardholders, Plaintiff Bellwether and the Florida Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff Bellwether and the Florida Class suffered an injury in Florida.

222. Chipotle willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the FDUTPA.

223. As a direct and proximate result of Chipotle's unfair practices and violation of FDUTPA, Plaintiff Bellwether and the Florida Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT SEVEN

Violation of the Maine Unfair Trade Practices Act, 5 M.R.S.A §§ 205-A, *et seq.*

(On Behalf of Plaintiff Bellwether and the Maine Class)

224. Plaintiff Bellwether incorporates and realleges each and every allegation contained above as if fully set forth herein.

225. Plaintiff Bellwether brings this claim on behalf of itself and the Maine Class pursuant to the Maine Unfair Trade Practices Act ("MUTPA"), 5 M.R.S.A. §§ 205-A, *et seq*.

226. Plaintiff Bellwether and the Maine Class are "persons" within the meaning of MUTPA. 5 M.R.S.A. § 206(2).

227. Defendant is engaged in "trade" and "commerce" within the meaning of MUTPA. 5 M.R.S.A. § 206(3).

228. The MUTPA prohibits unfair acts or practices in the conduct of trade or commerce. An "unfair practice" within the meaning of the MUTPA is one that offends established public policy or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers. In interpreting its provisions, the MUTPA requires consideration be given to interpretations by the FTC relating to § 5 of the FTC Act. *See* 5 M.R.S.A. § 207(1).

229. Chipotle engaged in unfair acts under MUTPA by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Chipotle's trade or business.

230. Chipotle's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of MUTPA because they constituted immoral, unethical,

oppressive, and unscrupulous activity; caused substantial injury to consumers and businesses; and provided no benefit to consumers or competition.

231. Chipotle's failure also was unfair within the meaning of MUTPA because its conduct undermined Maine public policy that personal and financial information be protected from unauthorized disclosure, as reflected in 10 M.R.S.A. § 1347-A.

232. Plaintiff Bellwether and the Maine Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

233. Chipotle's conduct harmed competition. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Bellwether and the Maine Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Bellwether and the Maine Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

234. Plaintiff Bellwether and the Maine Class have members located in Maine who used Plaintiff's and the Class's payment cards to purchase food for personal consumption from Chipotle and whose payment cards were impacted by the Data Breach. For these Maine-based cardholders, Plaintiff Bellwether and the Maine Class reimbursed them for fraudulent

transactions and/or reissued payment cards impacted by the Data Breach. Through these acts, Plaintiff Bellwether and the Maine Class suffered concrete and substantial injuries in Maine.

235. Chipotle willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the MUTPA.

236. As a direct and proximate result of Chipotle's unfair practices and violation of MUTPA, Plaintiff Bellwether and members of the Maine Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT EIGHT

Violation of the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ch. 93A, *et seq.*

(On Behalf of Plaintiff Bellwether and the Massachusetts Class)

237. Plaintiff Bellwether incorporates and realleges each and every allegation contained above as if fully set forth herein.

238. The Massachusetts Consumer Protection Act, Mass. Gen. Laws. Ch. 93A, *et seq*. ("Chapter 93A"), makes it unlawful to engage in any "unfair or deceptive acts or practices in the conduct of any trade or commerce" and, in interpreting its provisions, requires consideration be given to interpretations by the FTC relating to § 5 of the FTC Act. *See* Mass. Gen. Laws. Ch. 93A §§ 2(a) and (b).

239. Plaintiff Bellwether and the Massachusetts Class are "persons" within the meaning of Chapter 93A, § 1(a).

240. Defendant is engaged in "trade" and "commerce" within the meaning of Chapter 93A, § 1(b).

241. Chipotle engaged in unfair business practices prohibited by Chapter 93A §§ 2 and 11, by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Chipotle's trade or business.

242. Chipotle's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of Chapter 93A because they constituted immoral, unethical, oppressive, and unscrupulous activity; caused substantial injury to consumers and businesses; and provided no benefit to consumers or competition.

243. Chipotle's failure also was unfair within the meaning of Chapter 93A because its conduct undermined Massachusetts public policy that businesses protect personal and financial information as reflected in Mass. Gen. Laws. Ch. 93H, § 2; 201 CMR 17.00; and the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits unfair trade practices.

244. Plaintiff Bellwether and the Massachusetts Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

245. Chipotle's conduct harmed competition. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Bellwether and the Massachusetts Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Bellwether and the

Massachusetts Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

246. The actions and transactions constituting Chipotle's unfair acts and practices under this claim occurred primarily and substantially in Massachusetts under the pragmatic, functional analysis employed by courts because: (a) Chipotle's unlawful conduct was intended to and did impact payment card transactions in its stores located in Massachusetts; (b) members of the Massachusetts Class were located in Massachusetts and incurred losses and suffered damages there; (c) payment cards used by Massachusetts consumers were stolen at stores located there and the stolen information was used to commit fraud in Massachusetts; and (d) Chipotle's unlawful conduct interfered with trade or commerce in Massachusetts.

247. Plaintiff Bellwether and the Massachusetts Class have members located in Massachusetts whose payment cards were impacted by the Data Breach. For these Massachusetts-based cardholders, Plaintiff Bellwether and the Massachusetts Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff Bellwether and the Massachusetts Class suffered an injury in Massachusetts.

248. Chipotle willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of Chapter 93A.

249. As a direct and proximate result of Chipotle's unfair practices and violation of Chapter 93A, Plaintiff Bellwether and the Massachusetts Class have suffered and will continue

to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT NINE

Violation of New Hampshire Consumer Protection Act, N.H. Stat. §§ 358-A:1, *et seq.*

(On Behalf of Plaintiff Bellwether and the New Hampshire Class)

250. Plaintiff Bellwether incorporates and realleges each and every allegation contained above as if fully set forth herein.

251. Plaintiff Bellwether and New Hampshire are "persons" within the meaning of N.H. Rev. Stat. § 358-A:1(I).

252. Defendant is engaged in "trade" and "commerce" within the meaning of N.H. Rev. Stat. § 358-A:1(II).

253. The New Hampshire Consumer Protection Act ("NHCPA"), prohibits unfair acts or practices in the conduct of trade or commerce. An unfair practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers, offends public policy as established by law or by other established concepts of unfairness, and is of the type proscribed by the NHCPA, attaining the level of rascality that would raise an eyebrow of someone inured to the rough and tumble of the world of commerce. In interpreting its provisions, the NHCPA requires express consideration be given to interpretations by the FTC relating to § 5 of the FTC Act. *See* N.H. Rev. Stat. § 358-A:13.

254. Chipotle engaged in unfair business practices prohibited by the NHCPA by unreasonably adopting and maintaining data security measures that were inadequate to protect

Payment Card Data and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Chipotle's trade or business.

255. Chipotle's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of the NHCPA because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition.

256. Chipotle's failure also was unfair within the meaning of NHCPA because its conduct undermined New Hampshire public policy that personal and financial information be protected from disclosure, as reflected in N.H. Rev. Stat. § 359-C:2.

257. Chipotle's misconduct, as alleged herein, is of the type proscribed by the NHCPA, attaining the level of rascality that would raise an eyebrow of someone inured to the rough and tumble of the world of commerce, because the consequences of Chipotle's inadequate data security measures were entirely foreseeable, yet Chipotle chose to not implement even those most basic data security measures. By accepting payment cards, Chipotle represented to the public and to Plaintiffs and the Class that it would safeguard Payment Card Data. By knowingly implementing inadequate data security measures, Chipotle created a likelihood of confusion because the public, Plaintiffs, and the Class had no way of ascertaining the adequacy of Chipotle's data security measures.

258. Plaintiff Bellwether and the New Hampshire Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

259. Chipotle's conduct harmed competition. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Bellwether and the New Hampshire Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Bellwether and the New Hampshire Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

260. Plaintiff Bellwether is located in New Hampshire, and it and the New Hampshire Class have members located in New Hampshire whose payment cards were impacted by the Data Breach. For these New Hampshire-based cardholders, Plaintiff Bellwether and the New Hampshire Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff Bellwether and the New Hampshire Class suffered an injury in New Hampshire.

261. Chipotle willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the NHCPA.

262. As a direct and proximate result of Chipotle's unfair practices and violation of the NHCPA, Plaintiff Bellwether and the New Hampshire Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT TEN

Violation of the Vermont Consumer Fraud Act, 9 V.S.A §§ 2451, *et seq.*

(On Behalf of Plaintiff Bellwether and the Vermont Class)

263. Plaintiff Bellwether incorporates and realleges each and every allegation contained above as if fully set forth herein.

264. Plaintiff Bellwether and the Vermont Class are "consumers" within the meaning of 9 V.S.A. § 2451a(a) insofar as they agree to pay for services in connection with the operation of their business to enable their members to purchase goods from Chipotle with their payment cards.

265. Defendant is a "seller" within the meaning of 9 V.S.A. § 2451a(c).

266. The Vermont Consumer Fraud Act ("VCFA") prohibits unfair acts or practices in the conduct of trade or commerce. In interpreting its provisions, the VCFA requires express consideration be given to interpretations by the FTC relating to § 5 of the FTC Act. *See* 9 V.S.A. § 2453(b).

267. Chipotle engaged in unfair business practices prohibited by the VCFA by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Chipotle's trade or business.

268. Chipotle's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of the VCFA because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition.

269. Chipotle's failure also was unfair within the meaning of VCFA because its conduct undermined Vermont public policy that personal and financial information be protected from unauthorized disclosure, as reflected in 9 V.S.A. § 2435.

270. Plaintiff Bellwether and the Vermont Class reasonably expected Chipotle to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

271. Chipotle's conduct harmed competition. While Chipotle cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Bellwether and the Vermont Class are not outweighed by any countervailing benefits to consumers or competition. And, because Chipotle is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff Bellwether and the Vermont Class could have known about Chipotle's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Chipotle's legitimate business interests, other than its conduct responsible for the Data Breach.

272. Plaintiff Bellwether and the Vermont Class have members located in Vermont whose payment cards were impacted by the Data Breach. For these Vermont-based cardholders, Plaintiff Bellwether and the Vermont Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff Bellwether and the Vermont Class suffered an injury in Vermont.

273. Chipotle willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the VCFA.

274. As a direct and proximate result of Chipotle's unfair practices and violation of the VCFA, Plaintiff Bellwether and the Vermont Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT ELEVEN

Declaratory And Injunctive Relief

275. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

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

277. An actual controversy has arisen in the wake of the Chipotle Data Breach regarding its duty to reasonably safeguard Payment Card Data. Plaintiffs allege that Chipotle's data security measures were inadequate and remain inadequate. Chipotle likely will deny these allegations. Furthermore, Plaintiffs and the Class continue to suffer injury as additional fraudulent charges are being made on payment cards issued to Chipotle customers.

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

(a) Chipotle continues to owe a legal duty to secure Payment Card Data;

(b) Chipotle continues to breach this legal duty by employing inadequate and unreasonable measures to secure Payment Card Data; and

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

279. The Court also should issue corresponding injunctive relief requiring Chipotle to employ adequate security protocols, consistent with industry standards, to protect Plaintiffs' and the Class's Payment Card Data. Specifically, this injunction should, among other things, direct Chipotle to:

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

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

(c) implement EMV technology;

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

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

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

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

(h) utilize up-to-date POS hardware and software; and

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

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

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

282. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Chipotle, thus eliminating the injuries that would result to Plaintiffs and the Class whose Payment Card Data would be compromised.

PRAYER FOR RELIEF

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

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

B. monetary damages;

C. injunctive relief;

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

E. costs;

F. pre- and post-judgment interest; and

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

JURY DEMAND

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

DATED: October 30, 2017

s/ Joseph P. Guglielmo

Joseph P. Guglielmo
Carey Alexander
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Erin Green Comite
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
156 South Main Street
Colchester, CT 06415
Telephone: 860-537-5537
Facsimile: 860-537-4432
ecomite@scott-scott.com

Arthur M. Murray
Caroline T. White
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Telephone: 504-525-8100
Facsimile: 504-584-5249
amurray@murray-lawfirm.com

Interim Co-Lead Counsel for Plaintiffs

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: 612-339-7300
Facsimile: 612-336-2940
bbleichner@chestnutcambronne.com

Gary F. Lynch
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15212
Telephone: 412-322-9243
Facsimile: 412-231-0246
glynch@carlsonlynch.com

Karen H. Riebel
Kate M. Baxter-Kauf
Rachel M. Bohman
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: 612-339-6900
Facsimile: 612-339-0981

khriebel@locklaw.com

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

Brian C. Gudmundson
ZIMMERMAN REED, LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: 612-341-0400
Facsimile: 612-341-0844
brian.gudmundson@zimmreed.com

Plaintiffs' Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that on October 30, 2017, the foregoing document was filed using the Court's CM/ECF system, which will automatically generate electronic service upon registered counsel for all parties.

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo