IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION AT CLEVELAND

IN RE: SONIC CORP. CUSTOMER DATA BREACH LITIGATION (Financial Institutions)	)	MDL Case No. 1:17-md-02807-JSG
THIS DOCUMENT RELATES TO ALL FINANCIAL INSTITUTION ACTIONS	)	

AMENDED CLASS ACTION COMPLAINT

Plaintiffs American Airlines Federal Credit Union, Redstone Federal Credit Union, and Arkansas Federal Credit Union (collectively, "Plaintiffs"), by their undersigned counsel, file this Amended Class Action Complaint on behalf of themselves and a class of all similarly situated financial institutions and other entities against Sonic and its subsidiaries (collectively, "Sonic"). Plaintiffs base the following allegations upon personal information and belief, and the investigation of counsel:

INTRODUCTION

1. Sonic is a nationwide fast-food restaurant, unique for its drive-in experience. Most Sonic restaurants are franchise-owned, including around 94% of all Sonic restaurants in the United States. Despite the significant ratio of franchisee to corporate-owned restaurants, Sonic maintains strict control over the operation of franchises, including, specifically, infrastructure, technology and data security.

2. For instance, among other things, Sonic took responsibility for: [redacted] (7) training franchisees on new technology and point-of-sale systems, and (8) requiring franchisees to pay into a Brand Technology Fund ("BTF") that Sonic used to finance changes in technology and cybersecurity at franchisee restaurants. These requirements provide Sonic with significant oversight and control over franchises and ultimately, their state of cybersecurity.

3. For the purpose of ensuring adequate cybersecurity protections at franchisee restaurants, Sonic knew or should have known of the need to secure franchise point-of-sale ("POS") systems, those systems used to accept and process payment cards. Over the last five years, practically every major data breach involving retail stores or fast-food chains was caused by hackers accessing and placing malware directly on POS systems at stores or restaurants. Indeed, data security experts have repeatedly warned, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[1]

4. [redacted]

[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#.

[redacted].

5. Sonic also knew of data security measures capable of preventing or limiting the scope of a data breach involving POS systems. For example, Sonic was obligated to adhere to certain data security requirements set forth in the Payment Card Industry Data Security Standards ("PCI DSS"). PCI DSS was created by the Payment Card Industry, including Visa, MasterCard, American Express, Discover and JCB International (the "Card Brands"), to provide "technical and operational requirements . . . to protect card holder data" that applied to "all merchants organizations that store, process or transmit [payment card] data . . . ."[2] Because, at all relevant times, Sonic processed payment card data, Sonic was obligated by its agreements with the Card Brands to comply with PCI DSS.

6. In addition to PCI DSS compliance, the Federal Trade Commission ("FTC"), state governments, and data security organizations created industry standards and made recommendations designed to prevent and limit the scope of a data breach. Generally, these measures were more rigorous than the PCI DSS. One such standard, for example, was the ISO/IEC 27000 information security management system standard published by the Internal Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27000 was designed to provide standard best practices for implementing a comprehensive data security program, including implementing adequate security tools, security personnel, and security

[2] *Payment Card Industry Security Standards*, PCI SECURITY STANDARDS COUNCIL (Oct. 2010), https://www.pcisecuritystandards.org/documents/PCI_SSC_Overview.pdf?agreement=true&time=1560370308360

departments and creating a sufficient data security response program. Many data security analysts refer to these best practices when assessing a company's data security posture.

7. Moreover, the FTC has also made it clear to companies that accept payment card data that the failure to take reasonable security measures to protect the security and confidentiality of such data constitutes a violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. §45, and will be fined accordingly. *See*, *e.g.*, *F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. §45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

8. Given the highly publicized data breaches that have occurred over the past five years, [redacted], the PCI DSS, the data security best practices set forth by other independent organizations, and the FTC's approach to data security, Sonic fully knew its POS systems would be a target for hackers,

understood the vulnerabilities of its POS systems, and understood that, if not resolved, those vulnerabilities increased the likelihood of a data breach. Sonic also knew of reasonable data security measures that would prevent hackers from infiltrating its systems, prevent the application of malware on its POS systems, and allow for fast identification and remediation of any intrusion.

9. Despite Sonic's knowledge of the vulnerabilities of its POS systems, the consequences of a breach, and methods to secure its POS systems, it completely failed to prioritize its data security. Due to significant delays in implementing a technology revitalization plan that began in 2013, franchisees were left using significantly outdated and insecure systems. Indeed, Sonic recognized that some of these systems were more than 30 years old, and likened them to "rotary era" technology.[3] [redacted].

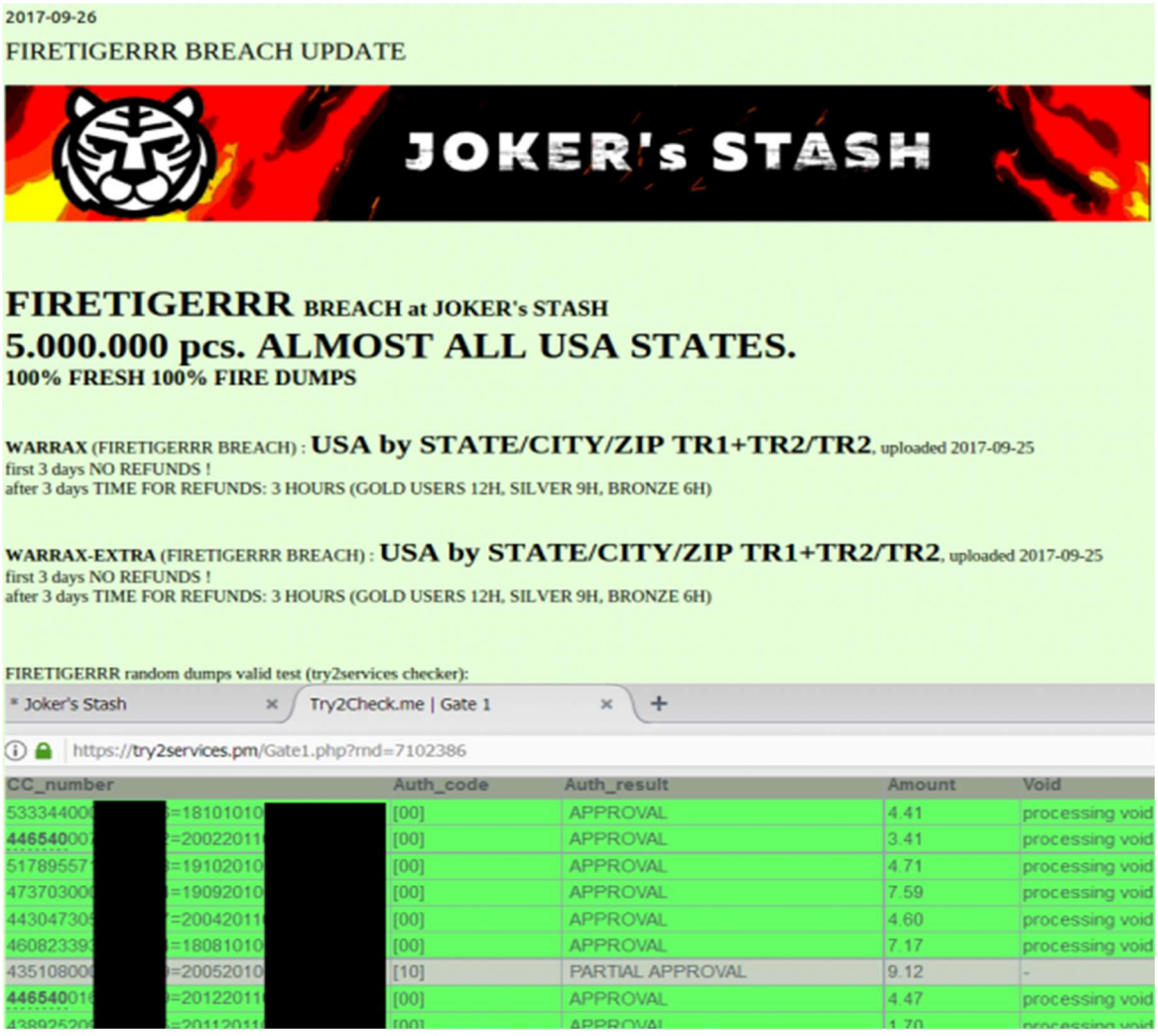
10. As a result of Sonic's insecure and outdated systems, from approximately April 2017 through October 2017, hackers breached certain Sonic restaurants, and for approximately six months collected customer payment card data [redacted] (the "Data Breach"). Over the course of the Data Breach, the hackers compromised approximately 5 million payment cards.

11. Sonic never identified the Data Breach. Instead, the Card Brands and the institution that processed Sonic's card payments warned Sonic that it may be experiencing a Data Breach based on investigations that found that Sonic was the common point-of-purchase of payment cards

[3] Ron Ruggless, *Sonic team helps operators reap benefits of new POS system*, Nation's Restaurant News (Apr. 14, 2017), https://www.nrn.com/technology/sonic-team-helps-operators-reap-benefits-new-pos-system.

(i.e. all payment cards had been recently used at a Sonic prior to the theft and sale of the card data) being sold on the dark web to fraudsters.

12. On September 18, 2018, data security expert, Brian Krebs reported that five million credit and debit card accounts were available for purchase on a "dark web" site called Joker's Stash and that such cards had been used at Sonic locations.[4] Krebs provided a screen shot of Joker's Stash, the website where the cards stolen from Sonic's restaurants were being sold:



[4] *See* Brian Krebs, *Breach at Sonic Drive-In May have Impacted Millions of Credit, Debit Cards*, KrebsOnSecurity (Sep. 26, 2017), https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/

13. [redacted].

14. [redacted].

15. [redacted] showed that Sonic's Data Breach was the predictable result of Sonic's inadequate data security measures and failure to prioritize data security. [redacted].

16. [redacted]. Sonic also deliberately chose not to implement EMV-capable POS systems, a payment card security feature required by the Payment Card Industry and recommended by security experts that would have prevented the re-use of stolen payment card information.

17. Had Sonic implemented reasonable data security processes and procedures, including those measures known and recommended by the Payment Card Industry, the FTC, and data security experts, Sonic could have reasonably prevented the breach of its systems and the resulting damage.

18. Sonic knew that a breach would cause significant harm to the financial institutions responsible for re-issuing compromised cards and reimbursing consumers for fraudulent transactions caused by a data breach. Indeed, when Sonic announced the Data Breach, it instructed customers that "[i]f you see any unauthorized activity, contact your financial institution." [5]

19. After a data breach involving payment cards, the Card Brands like Visa, Mastercard, AmericanExpress, and Discovery, typically issues alerts to financial institutions informing them that a data breach may have compromised one or more of their payment card accounts. Upon receipt of such an alert, Financial Institutions, like Plaintiffs and the Class, have a legal and business obligation to respond quickly to protect their customers against further harm.

20. After receiving an alert, financial institutions have a range of viable and reasonable responses. Card-issuing financial institutions are legally required to reimburse their customers for any fraudulent charges made with any payment card they issued. Therefore, to limit the amount of fraud on potentially compromised accounts, financial institutions take reasonable measures such as cancelling and reissuing the payment cards and increasing their monitoring for potentially fraudulent charges. Even where financial institutions do not reissue payment cards upon receipt of an alert, all financial institutions take some action to respond to the alert, which may include evaluating the risk to open accounts, increasing fraud monitoring, informing customers of a

[5] Notice of Data Breach, https://www.sonicdrivein.com/-/notice-of-data-breach (last visited Oct. 18, 2019).

potential breach of payment card information, performing investigations of the data breach, analyzing fraudulent charges, or taking any number of reasonable, accepted, and often required responses to an alert.

21. Many of these reasonable responses are taken to prevent future fraud and to ensure that customers are willing to continue to use their payment card accounts despite being potentially compromised by the Data Breach. Indeed, through no fault of their own, financial institutions' members typically use cards involved in a data breach less, resulting in decreased revenue for the financial institution. This incentivizes financial institutions to take immediate action upon receiving notification that payment accounts were affected by a data breach.

22. As a result of Sonic's Data Breach, Plaintiffs and the Class each received alerts notifying them that their payment card accounts were compromised. In response, Plaintiffs and the Class took measures to prevent further harm, including: (a) canceling or reissuing credit and debit cards affected by Sonic's Data Breach; (b) closing deposit, transaction, checking, or other accounts affected by Sonic's Data Breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) opening or reopening deposit, transaction, checking, or other accounts affected by Sonic's Data Breach; (d) refunding credit card holders to cover the cost of unauthorized transactions relating to Sonic's Data Breach; (e) responding to a higher volume of cardholder complaints, confusion, and concern; and/or (f) increasing fraud monitoring efforts. These measures caused substantial damages to each of the Plaintiffs.

23. As alleged herein, the injuries to Plaintiffs and the Class were directly and proximately caused by Sonic's failure to implement and maintain adequate and reasonable data security measures necessary for protecting customer information, including credit and debit card data. Sonic failed to take steps to employ adequate security measures despite well-publicized data

breaches at large national retail and restaurant chains in the months and years preceding the Data Breach, including Target, Home Depot, P.F. Chang's, Eddie Bauer, Wendy's, Dairy Queen, Noodles & Co., Arby's, Chipotle and Kmart.

24. This class action is brought on behalf of financial institutions throughout the United States to recover the costs that they have been forced to bear as a direct result of the Data Breach of Sonic's systems and to obtain other equitable relief. Plaintiffs assert claims for negligence, negligence per se, and for declaratory and injunctive relief.

JURISDICTION AND VENUE

25. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332 (d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and at least some members of the proposed Class have a different citizenship than Sonic.

26. This Court has personal jurisdiction over Sonic because Sonic conducts substantial business in this District, maintains restaurants in this District, and has sufficient minimum contacts in Ohio. Sonic intentionally availed itself of this jurisdiction by accepting and processing payments for its services and goods within Ohio.

27. Venue is proper under 18 U.S.C. § 1391(a) because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

28. **Plaintiff** American Airlines Federal Credit Union ("AAFCU") is a Credit Union headquartered in Fort Worth, Texas. AAFCU issues payment cards to its members, who in turn use those payment cards for purchases. AAFCU suffered injury as a result of the Sonic Data Breach. AAFCU received eight alerts notifying it of nearly 7,000 payment card accounts identified

as compromised due to the Sonic Data Breach. AAFCU estimates it incurred tens of thousands of dollars' worth of damages responding to the Data Breach, including cancelling and reissuing impacted cards, reimbursing customers for fraudulent transactions on alerted-on cards, increased fraud monitoring, and other time spent responding to the Data Breach.

29. **Plaintiff** Redstone Federal Credit Union ("Redstone") is headquartered in Huntsville, Alabama and, with over 400,000 members, is Alabama's largest credit union. Redstone operates 26 branches in Alabama and Tennessee and was ranked the 21st largest federal credit union in the United States by assets and the 17th largest credit union by membership. Redstone issues payment cards to its members, who in turn use those payment cards for purchases. Redstone suffered injury as a result of the Sonic Data Breach. Redstone received eight alerts listing nearly 50,000 payment card accounts compromised as a result of the Sonic Data Breach. Redstone estimates it incurred approximately $1 million worth of damages responding to the Data Breach, including cancelling and reissuing payment cards, reimbursing customers for fraudulent transactions on alerted-on cards, and other administrative costs incurred in investigating and responding to the Data Breach (e.g., paying employees overtime to timely perform tasks related to Redstone's response to the Data Breach).

30. **Plaintiff** Arkansas Federal Credit Union ("Arkansas FCU") is headquartered in Jacksonville, Arkansas and serves over 108,00 members across 15 branches. Arkansas FCU is the largest credit union in the State of Arkansas, primarily serves Arkansas residents, and is a significant contributor to the Arkansas community. Arkansas FCU issues payment cards to its members, who in turn use those payment cards for purchases. Arkansas FCU suffered injury as a result of the Sonic Data Breach. Arkansas FCU received seven alerts notifying it of approximately 6,300 payment card accounts compromised by the Sonic Data Breach. Arkansas FCU estimates it

incurred tens of thousands of dollars' in damages responding to the Data Breach, including cancelling and reissuing cards, reimbursing customers for fraudulent transactions on alerted-on cards, monitoring for fraud, and performing other administrative tasks (e.g., communicating with customers about the Data Breach).

31. **Defendant** Sonic Corp. is a Delaware corporation with its principal place of business or "World Headquarters" at 300 Johnny Beach Dr., Oklahoma City, OK, 73104.

32. **Defendant** Sonic Industries Services, Inc. is a subsidiary of Sonic Corp. and is an Oklahoma corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma.

33. **Defendant** Sonic Capital LLC is a subsidiary of Sonic Corp. and is a Delaware limited liability company with its principal place of business in Oklahoma City, Oklahoma.

34. **Defendant** Sonic Industries LLC is a subsidiary of Sonic Corp. and is a Delaware limited liability company with its principal place of business in Oklahoma City, Oklahoma.

35. **Defendant** Sonic Franchising LLC, is a subsidiary of Sonic Corp. and is a Delaware limited liability company with its principal place of business in Oklahoma City, Oklahoma.

36. **Defendant** Sonic Restaurants, Inc. is a subsidiary of Sonic Corp. and is an Oklahoma corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma.

ALLEGATIONS

37. Sonic is America's most successful fast food drive-in restaurant. By sales alone, Sonic is the twelfth largest restaurant chain in the United States and the fourth largest quick service restaurant chain. Since 2013, Sonic has averaged over half a billion dollars in total revenue annually from both its franchise and corporate restaurants.

38. Most of Sonic's restaurants are franchise-owned. Of the nearly 3,600 Sonic restaurants dispersed through 45 different U.S. states, 94% are franchise-owned and only 6% are corporate owned. Sonic's business model is to permit franchisees to operate Sonic restaurants while Sonic retains control over aspects of the brand, including control over technology and customer experience. To that end, all franchisees are required to comply with Sonic's strict operating criteria outlined in franchisee license agreements, Sonic's operating manual, and other policies issued by Sonic.

39. [redacted].

40. [redacted].

41. [redacted]

[redacted].

42. [redacted].

43. Sonic also established a BTF which was purportedly established to pay for "cybersecurity and other technology programs for Sonic systems" at both franchise-owned and corporate owned restaurants.[6] Sonic funded the BTF, in part, by requiring franchisees to pay technology fees directly to Sonic.[7] The BTF allowed Sonic to fund, control, and ensure the uniformity of franchisee technology and data security. Using the BTF, Sonic had the authority to unilaterally determine which technologies and security measures it would fund and franchisees would have to adopt.

44. In 2013, using the BTF, Sonic began plans to implement a full technology revitalization of its in-store and mobile technologies, including new POS systems that were "designed to boost profitability through improved food cost and labor management" and a Point of Personalized Service platform involving new digital menu boards integrated with mobile and

[6] Annual Report, Sonic at 31 (2016), http://www.annualreports.com/HostedData/AnnualReportArchive/s/NASDAQ_SONC_2016.pdf.

[7] *Id.*

other digital efforts.[8] Sonic Corporate led the effort and unilaterally selected which technologies would be included in the revitalization plan at all franchise-owned and corporate-owned restaurants.

45. The technology revitalization plan was desperately needed. Sonic acknowledged that its new POS systems were replacing systems that were more than 30 years old.[9] As Matt Schein, Sonic's Vice President of Operations publicly admitted, "we kind of went from a rotary phone to a smartphone overnight." The fact that many of Sonic's POS systems were decades old was a massive failure considering the fast growing and advanced hacking techniques that have developed over the past decade alone.

46. Despite the risk these "rotary era" technologies posed, Sonic gave no urgency to its technology revitalization. Although Sonic began the revitalization in 2013, it had failed to fully implement the plan by 2017, four years after its inception and long after its target completion date in 2016.[10] By the end of 2017, Sonic had only converted 77% of its POS systems under the revitalization plan. The remaining 23% of restaurants continued to use older systems, terminals, and data security measures. [redacted].

47. These outdated measures left franchisees vulnerable. [redacted]

[8] Kara Murphy, *Sonic Rolls Out New POS and POPS Systems*, Retail Insights (Jan. 16, 2014), https://www.retailitinsights.com/doc/sonic-rolls-out-new-pos-and-pops-systems-0001.

[9] Zorrik Voldman, *Sonic Drive-In Is Victim to Security Breach*, 911 Software (Oct. 20, 2017), https://www.911software.com/sonic-drive-in-is-victim-to-security-breach/.

[10] *See* Murphy, *supra* note 8.

[redacted].

48. [redacted].

49. [redacted].

50. [redacted][11]

[11] "A cardholder data environment (CDE) is a computer system or network group of [infrastructure technology) systems that processes, stores, and/or transmits cardholder data or sensitive payment authentication data," and typically including point-of-sale systems. *Cardholder Data Environment (CDE)*, TechTarget.com (last visited, Jan. 2, 2019), https://searchsecurity.techtarget.com/definition/cardholder-data-environment-CDE

[redacted].

51. Sonic's "rotary era" technology used at franchise-owned restaurants, its deficient data security measures, and its strict control over franchisee configurations put franchisees at significant risk of a data breach. Sonic acknowledged this fact by recognizing as early as 2013 that it needed to completely replace franchisee POS systems. [redacted].

52. Despite Sonic's awareness of the vulnerabilities at franchise-owned restaurants, it wholly failed to adequately and timely address them. As a result, Sonic suffered a massive Data Breach resulting in the preventable theft of payment card data from millions of credit and debit cards used at Sonic restaurants. [redacted], collecting customer payment card data at will. Throughout the nearly six-month long Data Breach, Sonic allowed hackers to access millions of customers' payment card information through malware that infected systems [redacted].[12]

Sonic's Data Breach Foreseeably Resulted from its Significant Security Deficiencies

53. Starting on April 7, 2017, hackers infiltrated Sonic's POS systems [redacted].

[12] *See* Krebs, *supra* note 4.

54. A POS system provides the hardware, software, and networks responsible for facilitating payments made by credit and debit cards. At a POS terminal, "data contained in [a payment] card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[13] The payment processor completes the transaction by passing payment information to the appropriate Card Brand (Visa, MasterCard, etc.) networks and then to the financial institution that issued the card for approval of the transaction (the "issuing bank").[14] Once approved, the retailer is paid by its acquiring or merchant bank, and the issuing bank later reimburses the acquiring bank for the transaction.

55. To send payment card information to the payment processor, businesses use a CDE.[15] The CDE is the part of the POS network that transfers card information from the POS terminal to the payment processor, which in turn assists with authorizing the transactions. Elements of the CDE include all network components like firewalls, switches, routers, access points, and network appliances, POS systems, servers, and often virtual components like virtual machines, switches, routers, desktops and hypervisors.

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

[14] Slava Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions 8 (Wiley 2011).

[15] *Cardholder Data Environment*, *supra* note 11 (noting "[m]ost data breaches in the retail sector involve a compromise of the cardholder data network.").

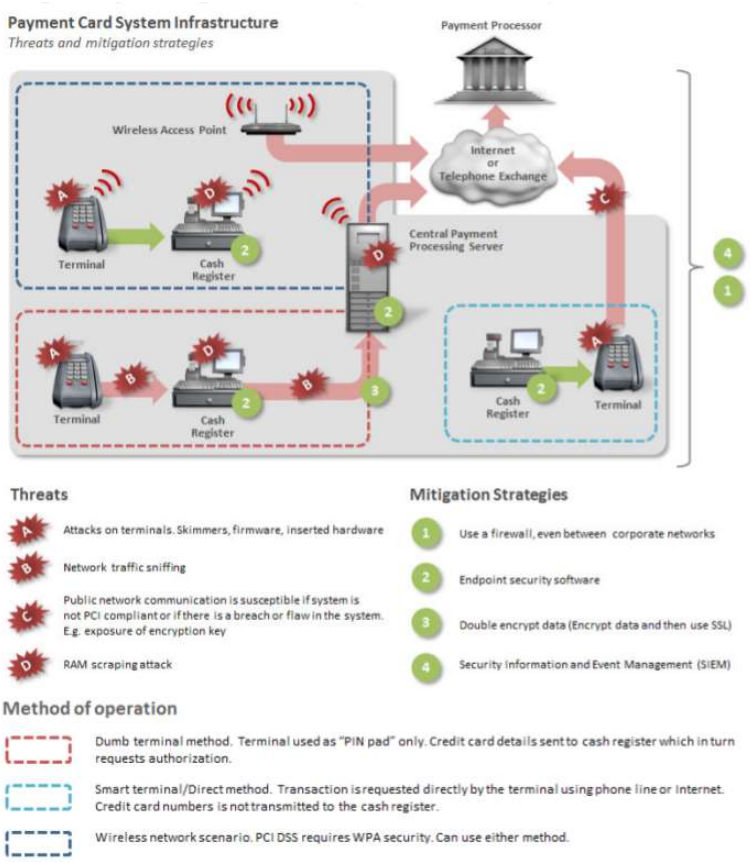


Figure 1. **An example of a CDE and its vulnerabilities.**

56. When hackers gain access to restaurant CDEs, including POS systems, they have direct access to payment card information. Before transmitting consumer purchasing information over the network through the deployment architecture, the POS system typically, very briefly, stores data from the card's magnetic stripe in unencrypted plaintext within the POS system's memory before transfer or encryption.[16] Stored payment information includes "Track 1" and "Track 2" data—originally stored on the magnetic stripe of the payment card—which includes full information about the cardholder, including first and last name, the expiration date of the card, and the CVV (three number security code on the card).[17] This information is unencrypted on the card

[16] Symantec, *supra* note 15, at 6.

[17] Gomzin, *supra* note 16, at 98-101.

and, if left unencrypted on the POS device, is easily accessible by hackers using common malware.[18] Hackers with access to Track 1 and Track 2 payment card data can physically replicate the card for in-person use or can use the data to make fraudulent purchases online.

57. [redacted], hackers collected and exfiltrated customer payment card data for over six months completely unnoticed by Sonic. Indeed, Sonic never discovered the breach itself. Rather, on September 19, 2019, the Card Brands and [redacted], notified Sonic that their investigations had linked Sonic to certain payment card data for sale on a website called "Joker's Stash," a site on the "dark web" notorious for selling stolen payment card data to fraudsters.

58. The Card Brands required Sonic to perform a PCI forensic investigation ("PFI") to determine whether Sonic was experiencing a Data Breach and, if so, remediate and contain the breach. In addition to its investigation of the Data Breach, the PFI investigator would review and report on Sonic's compliance with the PCI DSS, the minimum data security standards required by the Payment Card Industry to accept payment cards.

59. [redacted].

60. [redacted]

[18] Symantec, *supra* note 15, at 5.

[redacted].

61. [redacted].

62. [redacted].

63. [redacted]

[redacted].

64. [redacted].

65. [redacted].

66. Prior to the Data Breach, Sonic had also chosen not to implement "EMV" (Europay Mastercard and Visa), which is a type of physical payment card on which payment information is generated by a computer chip embedded within the card. Unlike magnetic stripe cards that use static data (i.e. the card information never changes), EMV cards use dynamic data for which a unique transaction code is created for each transaction and cannot be used again. When payment card information from an EMV transaction is stolen, the unique payment information typically cannot be used by the hackers, making it much more difficult for criminals to profit from what is

stolen. Despite the benefits of EMV, Sonic's Vice President of Public Relations, Christi Woodworth, stated that Sonic "ha[d] not adopted EMV for a variety of reasons specific to our business."[19]

67. [redacted].

68. [redacted].

69. [redacted].

70. [redacted].

[19] Jeremy Kirk, *Fast-Food Chain sonic Investigates Potential Card Breach*, Bank Info Security (Sep. 27, 2017), https://www.bankinfosecurity.com/sonic-drive-in-investigating-possible-card-breach-a-10337

71. [redacted].

72. [redacted].

73. [redacted]

[redacted].

74. Sonic's public response to the breach was likewise inadequate. The first public information about the Sonic breach came from a data security expert and blogger, Brian Krebs.[20] Krebs reported that multiple banks had determined that about five million credit cards placed on "Joker's Stash" had a common point of purchase at Sonic restaurants.

75. Krebs contacted Sonic to inform it of the potential Data Breach, and Sonic confirmed to Krebs that it was investigating the Data Breach of its POS systems. Sonic wrote:

> Our credit card processor informed us last week of unusual activity regarding credit cards used at SONIC . . . The security of our guests' information is very important to SONIC. We are working to understand the nature and scope of this issue, as we know how important this is to our guests. We immediately engaged third-party forensic experts and law enforcement when we heard from our processor. While law enforcement limits the information we can share, we will communicate additional information as we are able.[21]

76. Although its investigation of the Data Breach began nearly three weeks earlier and it knew payment cards used at Sonic were for sale to fraudsters on the dark web, Sonic waited until October 4, 2017 to provide any public notice. However, Sonic's notices casted doubt on whether the Data Breach resulted in the theft of payment cards, stating "credit and debit card numbers *may* have been acquired without authorization."[22] At that time, Sonic provided no information about

[20] Krebs, *supra* note 4.

[21] *Id.*

[22] Plaintiffs' Amended Consolidated Class Action Compl., *In re: Sonic Corp. Customer Data Breach Litig.*, 17-md-02807-JSG, ECF 114 ¶ 47 (N.D. Ohio, July 27, 2018) ("Consumer Compl.").

the scope or extent of the Data Breach and did not indicate which restaurant locations were impacted.

77. Sonic waited five months to announce which Sonic locations had been impacted by the Data Breach.[23] Sonic then issued a revised notice of the Data Breach, listing the addresses of 325 locations that it identified as compromised even though [redacted].[24]

78. Sonic's inadequate data security measures and response to the Data Breach appears to be the result of its business culture. One anonymous individual claiming to be a former Sonic employee recounted that Sonic's "[a]ntiquated Software caused [the] Breach."[25] The individual wrote that Sonic's "[e]xecutives [were] too focused on delivering unnecessary . . . 'new apps' instead of fixing a problem they were all aware of, [and the] end result [is] millions of customers impacted, [s]tock prices go down, more layoffs to come[.]"[26] The individual's view aligns with Sonic's repeated emphasis on new technologies but complete lack of security-driven projects.

79. The Sonic breach may have continued even longer if Payment Card Industry investigators had not noticed unusual activity on payment cards used at Sonic restaurants, or if those investigators had not linked stolen credit card information on the internet to Sonic locations. In other words, Sonic was entirely oblivious to the breach until outside third parties informed it of the breach.

---

[23] *Id.* at ¶ 49.

[24] *See* Notice, *supra* not 5.

[25] *Sonic Corp. Layoffs*, The Layoff (last visited Dec. 4, 2018), https://www.thelayoff.com/t/PLisqcZ

[26] *Id.*

80. Ultimately, Sonic unreasonably failed to enact basic data security measures, and this failure permitted hackers to easily enter its franchise CDEs and POS Systems. Then, because Sonic failed to monitor its systems, the breach continued unnoticed for months until an estimated 5 million payment cards were compromised. The Sonic Data Breach and the resulting payment card theft would have been prevented had Sonic implemented reasonable, industry-recommended data security standards. However, it failed to do so.

Sonic Had Notice of the Need to Protect POS Systems

81. Sonic knew, or should have known, that vulnerabilities in its POS systems and the configurations it set up at franchise-owned restaurants would be targeted by hackers and leave franchise restaurants susceptible to a Data Breach.

82. Security experts have consistently warned about the susceptibility of POS systems in restaurants.[27] POS systems are known to be a preferred target of hackers seeking to collect payment card data. Indeed, data security experts have warned business that "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[28] The same article notes that Verizon reported "99 percent of the time, POS environments were hacked in only a few hours . . . [and] in 98 percent of cases, hackers exfiltrated data in just a couple of days." The reason for the number and significance of data breaches was "[s]imply put, too many businesses . . . practicing less-than-stellar POS security."[29]

---

[27] *5 Lessons To Learn From A Restaurant POS Security Breach*, Pointofsale.com (last visited, Feb. 28, 2017), https://pointofsale.com/201506256716/Restaurant/Hospitality/5-Lessons-to-Learn-from-a-Restaurant-POS-Security-Breach.html.

[28] *See* Datacap Systems, *supra* note 1.

[29] *5 Lessons*, *supra* note 27.

83. One expert warned businesses that "you can't neglect POS system security," noting that "[a]ny POS terminal with an IP address and a connection to a business's network is as vulnerable to compromise as all the other pieces of equipment in that network."[30] The same expert stated "[i]t's not only okay to be obsessive about testing your POS systems for vulnerabilities and compromises…it's essential."[31]

84. Additionally, data security experts have specifically and publicly warned businesses, like Sonic, about the threats of data breaches in the quick-service food industry. One expert warned that "overall fraud rates [in the food service industry] have risen by 13 percent since [2016]."[32] "[T]he threat is serious. Beyond POS systems, fraudsters often go directly to the source by attacking the restaurant's network or computer system, which stores files containing sensitive financial details. POS network attacks can affect multiple chain locations simultaneously and expose immense quantities of data in one fell swoop, allowing attackers to remotely steal data from each credit card as it is swiped at the cash register."[33] However, these data breaches are preventable: "To help prevent fraud attacks, restaurants need to ensure they comply with the standards governing the handling of payment card information, . . . manage the risks associated with third party vendors and put an effective incident response plan into place."[34]

85. In 2015, the National Restaurant Association warned restaurants that hackers "prey on businesses that are ill-prepared for an attack" and advised that "[j]ust as you have made food

[30] *Id.*

[31] *Id.*

[32] Michael Reiblat, *Is your restaurant data-breach proof?*, Fast Casual (Aug. 3, 2018), https://www.fastcasual.com/blogs/is-your-restaurant-data-breach-proof.

[33] *Id.*

[34] *Id.*

safety an integral part of your quality assurance program, you need to also make cybersecurity a part of your operation."[35] The Association admonished that "you're never finished" improving data security measures.[36] "[C]ybersecurity is not about checking boxes . . . Rather, cybersecurity is a continual process that you need to build into your daily operations. Threats will change, but if your cybersecurity program is designed properly, you'll be able to respond accordingly and adopt new policies to reduce the risk of cyberattacks. Remember, there are no shortcuts."[37]

86. Moreover, the theft of payment card information via POS systems has long been "one of the biggest sources of stolen payment cards."[38] According to one report, "[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data."[39] Hackers, on average, successfully compromise unsecured POS systems in a matter of minutes or hours, and are able to and exfiltrate data within days of placing malware on the POS devices.[40]

87. Since 2013, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet or chain restaurant. In 2015 alone, data breaches into POS systems accounted for 64% of *all* breaches where hackers successfully stole data.[41] In 2014,

---

[35] *Cybersecurity 101: A Toolkit for Restaurant Operators*, Nat'l Restaurant Assoc. 1 (2016), https://www.restaurant.org/Downloads/PDFs/advocacy/cybersecurity101.pdf.

[36] *Id.* at 4.

[37] *Id*.

[38] Symantec, *supra* note 15, at 3.

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

[40] *Id.* at 4.

[41] *Id.* at 3.

retail entities replaced credit, banking and financial institutions as the leader in the number of data breaches experienced per year and by far the most common means of data theft is through hacking, phishing, or skimming schemes targeting POS systems.[42]

88. [redacted].

89. These breaches have resulted in hundreds of millions of compromised payment cards,[43] and the number of breaches has continued to increase.[44] Since the 2014 Target Data Breach, the media has reported data breaches at numerous businesses and other chain restaurants, including: Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang's China Bistro, Eddie Bauer, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John's, Dairy Queen Restaurants, Staples, Kmart, Noodles & Co., GameStop, Wendy's, Chipotle and Arby's, among others.

90. The Wendy's data breach in particular should have been a massive warning sign for Sonic that it was vulnerable to a breach. In 2016, hackers compromised Wendy's Restaurants' POS systems using malware capable of stealing consumer purchasing information. Hackers gained entry into Wendy's POS machines at franchise-owned restaurants through methods similar to those used in the Target breach: compromised credentials provided to a third party service

[42] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScourt*, Identity Theft Resource Center (Jan. 19, 2017), http://www.idtheftcenter.org/2016data-breaches.html.

[43] Symantec, *supra* note38, at 3.

[44] *See* Identity Theft Resource Center, *supra* note 42.

provider with remote access to Wendy's franchise networks and restaurants.[45] Once hackers had access to Wendy's networks, they deployed malware onto POS terminals at franchise-owned locations, which ultimately collected consumer payment data.[46] At least one security expert believed that EMV chip readers (which Sonic decided not to use) at franchisee locations would have prevented some theft of payment data.[47] Although Wendy's discovered that its franchise-owned restaurants had been breached, it failed to determine the full scope of the breach and as a result failed to fully remediate the data breach. For more than six months, hackers stole payment card information from certain Wendy's franchise-owned restaurants before Wendy's fully identified and remediated the breach.[48] The relationship between Wendy's Corporate and Wendy's franchisees created vulnerabilities in the data security of Wendy's as a whole. Because Sonic Corporate similarly manages primarily franchise-owned systems and directs those restaurants' data security measures, the severity and scope of Wendy's data breach should have put Sonic on notice of the vulnerability of its own operations.

91. The Wendy's data breach, the data breaches at numerous other restaurants, and the specific warnings by data security experts put Sonic on notice that it was susceptible to its Data Breach and that it was crucial to prioritize data security in order to prevent a breach.

Sonic Knew of the Reasonable Measures Capable of Protecting Payment Card Data

92. Additionally, Sonic knew or should have known of specific recommended measures and businesses practices that reduce the likelihood that hackers can successfully intrude

---

[45] *Wendy's Update on Payment Card Security Incident*, Wendys.com (last visited, Apr. 26, 2017), http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2182670

[46] *Id.*

[47] Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KrebsOnSecurity (July, 16, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/#more-35408.

[48] *Id*.

into businesses' POS systems and that limit the effect of any malicious software installed on POS systems or devices. In fact, the Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, revealed in its 2015 annual report that 90% of data breaches in 2014 were preventable.[49] Similarly, in 2017, the Online Trust Alliance found more than 93% of incidents in 2016 were preventable.[50] The OTA emphasized that "[o]rganizations must make security a priority" and "those that fail will be held accountable."[51]

93. More than three years ago, a Symantec report listed vulnerabilities in POS systems that should be resolved to prevent entry into POS systems and theft of consumer purchasing information.[52] First, Symantec recommended "point to point encryption" implemented through secure card readers. These readers encrypt credit card information in the POS system, and prevent the installation of "RAM-scraping" malware ([redacted]), which extracts card information through the POS memory while it processes the transaction. Second, Symantec highlighted the need to utilize updated software to avoid susceptibility in older operating systems that are likely to be phased out by the manufacturers, such as Windows XP or Windows XP Embedded- ([redacted]). Third, Symantec emphasized the need to implement POS systems capable of accepting EMV chips in payment cards, which prevents the direct transmission of credit card information. Sonic's Vice

[49] Press Release, *OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented*, Online Trust Alliance (Jan. 21, 2015), https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented.

[50] Bradley Barth, Report: Number of Cyber Incidents Doubled in 2017, Yet 93 Percent Could Easily Have Been Prevented, SC Media (Jan. 28, 2018), https://www.scmagazine.com/home/security-news/privacy-compliance/report-number-of-cyber-incidents-doubled-in-2017-yet-93-percent-could-easily-have-been-prevented/

[51] Online Trust Alliance, *supra* note 49.

[52] *See* Symantec, *supra* note 15, at 11-12.

President of Public Relations stated that Sonic rejected this measure outright for "reasons specific to [Sonic's] business." These basic data security measures, known long before the Sonic Data Breach, are still important for preventing data breaches today.

94. The Payment Card Industry has also heightened security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

95. The PCI Security Standards Council, founded by American Express, Discover, JCB, MasterCard, and VISA, promulgates data security standards, known as PCI DSS, to "encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures." PCI DSS applies "to all entities involved in payment card processing," including merchants, processors, acquirers, issuers, and service providers. PCI DSS comprises "a minimum set of requirements for protecting data."[53]

96. PCI DSS 3.1 and 3.2, the versions of the standards in effect at the time of the Sonic Data Breach, set forth twelve detailed and comprehensive requirements that must be followed to meet six data security goals:

[53] *Requirements and Security Assessment Procedures*, PCI Security Standards Council at 5 (last visited Jun. 17, 2019), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1560805191237.

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps th mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

97. PCI DSS v. 3.1 and 3.2 created specific requirements for the types of software and security tools businesses must use, including antivirus and anti-malware software, security tools that track and monitor access to network resources and cardholder data, and methods of encrypting stored or transmitted cardholder data. Additionally, PCI DSS requires certain system configurations to limit the ability of unauthorized intruders to move across networks and firewalls and to prevent intruders from compromising administrative accounts by obtaining user names and passwords. PCI DSS also established rules specifically designed to protect CDE and POS systems.

98. The Payment Card Industry requires businesses to regularly analyze and test their data security measures to ensure they function properly and to identify security vulnerabilities.

Sonic and its franchisees are required to perform these tests annually and submit reports detailing the status of their PCI compliance to the PCI Council.

99. While meeting the mandatory PCI DSS requirements is an important first step to a reasonable cybersecurity posture, PCI DSS comprises only a portion of the minimum protective measures a business must take. As the PCI Council, which sets the PCI DSS requirements, acknowledges, PCI DSS represents the "minimum set of requirements for protecting account data," and it is widely recognized that PCI compliance alone is insufficient to prevent a data breach. The FTC, for example, warns that "PCI DSS certification is insufficient in and of itself to establish the existence of reasonable security protections. The [FTC's] *Wyndham* order calls for a number of additional signification protections . . . In short, the existence of PCI DSS certification is an important consideration in, but by no means the end of, our analysis of reasonable security."[54] In fact, "every company that has been spectacularly hacked in the last three years has been PCI compliant." Target, Home Depot, Neiman Marcus, Wendy's, Arby's, Michael's, Sally Beauty, Supervalu, Albertson's, and many other businesses subjected to data breaches were recognized as PCI DSS compliant at the time of the compromise.

100. To supplement PCI DSS and enhance data security requirements, federal and state governments have introduced security standards and recommendations to prevent data breaches and mitigate the resulting harm to consumers and financial institutions. The FTC has issued numerous guidelines for businesses highlighting the importance of reasonable data security

[54] *See* Statement of the Federal Trade Commission (FTC) v. Lifelock, FED. TRADE COMM'N (Dec. 17, 2015), https://www.ftc.gov/system/files/documents/public_statements/896143/151217lifelockcommstmt.pdf.

practices. The FTC notes the need to factor data security into all business decision-making.[55] According to the FTC, data security requires (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[56]

101. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

102. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network

[55] Federal Trade Comm'n, *Start With Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[56] *See id;* Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders further clarify the measures businesses must take to meet their data security obligations.

103. Several states have specifically enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as Cal. Civ. Code §1798.81.5(b) and Wash. Rev. Code §19.255; or that otherwise impose data security obligations on merchants, such as the Minnesota Plastic Card Security Act, Minn. Stat. §325E.64. Additionally, some states' unfair and deceptive trade practices acts include the failure to employ reasonable security processes to protect payment card data in the scope of prohibited unfair trade practice. Oklahoma's consumer protection statute, for example, prohibits business from "commit[ing] an unfair or deceptive trade practice." 15 OK Stat. § 15-753(20). Most states, including Oklahoma, have also enacted statutes requiring merchants to provide notice to consumers of security systems breaches. *See* 24 OK Stat. § 24-163. These statutes, implicitly or explicitly, mandate the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

104. As a result of the recommendations by data security experts, PCI DSS requirements, FTC requirements and recommendations under Section 5 of the FTC Act, and other federal and state data security requirements, Sonic was fully on notice of both need to implement

reasonable data security measures to prevent its Data Breach and the risk posed by unsecured CDEs and security measures.

The Sonic Data Breach Harmed Financial Institutions

105. In this case, Sonic was at all times fully aware of its data protection obligations for all Sonic franchise-owned and corporate restaurant locations because of, among other things, its participation in payment card processing networks. Sonic also knew of the significant repercussions of a data breach because of the numerous daily transactions involving tens of thousands of sets of payment card data. Sonic further knew that because they accepted payment cards at Sonic restaurant locations that processed sensitive financial information, customers and financial institutions, including Plaintiffs and the Class, were entitled to and did rely upon Sonic to keep sensitive information secure from hackers.

106. At all relevant times, Sonic was aware that the payment card data it receives via credit and debit card transactions is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. Sonic knew of the necessity of safeguarding payment card data and of the foreseeable consequences that would occur if its data security systems were breached, including the significant costs that would be imposed on issuers, such as the Plaintiffs and the Class. Numerous widely-reported retail and fast-food chain data breaches put Sonic on notice of the means by which hackers infiltrate POS systems and obtain payment card data.

107. Despite understanding the consequences of a data breach and the measures it could take to avoid a data breach, Sonic failed to comply with PCI DSS requirements; failed to take additional protective measures beyond the PCI DSS; failed to implement EMV-capable POS systems by the October 1, 2015 deadline; operated POS systems with outdated operating systems

and software; failed to enable point-to-point and end-to-end encryption; and failed to take necessary protective measures on its corporate network.

108. The culmination of Sonic's failed security measures was the Data Breach, which resulted in the intrusion of franchise CDEs and POS systems and allowed hackers to compromise [redacted] and resulting in the theft of information on over 5 million payment cards.

109. Sonic failed to reasonably protect cardholder information, putting consumer financial accounts in jeopardy and forcing financial institutions, like Plaintiffs and the Class, to take costly remedial action.

110. Financial institutions, like Plaintiffs and the Class, have a legal and business obligation to respond quickly to any notice of a payment card potentially compromised in a data breach. Upon learning of a breach that likely impacted its customers and/or receiving notice of a potentially compromised accounts, usually from the Card Brands, financial institutions have a range of viable and reasonable responses.

111. In most cases, card-issuing financial institutions are legally required to reimburse their customers for any fraudulent charges made with any payment card they issued. To limit the amount of fraud on a potentially compromised account, financial institutions take reasonable measures such as cancelling and reissuing the payment card and increased monitoring for potentially fraudulent charges.

112. Additionally, financial institutions often expend significant amounts of time and money keeping their customers informed about the potential effects of a data breach and fielding inquiries from concerned customers seeking information about their personal and financial information. When personal information and payment card data is stolen, as in the Sonic Data Breach, hackers can make wide use of that data for fraudulent purposes. For example, hackers sell

payment card data on the dark web at sites such as "Joker's Stash," where cards stolen from Sonic were available for purchase. Fraudsters purchase this data and then either duplicate the card to be swiped at in-store locations for fraudulent purposes or commit card-not-present fraud, in which payment card information is used to make online purchases without the need for a physical card.

113. Given the massive fraud that occurs in the wake of a data breach, financial institutions must act swiftly to protect their reputations with their customers and their bottom lines. Financial institutions have a strong incentive to keep the payment cards they issue at the "top of the wallet," which requires them to maintain customers' confidence and willingness to use their payment cards frequently. Due to no fault of the financial institutions, however, customers of financial institutions potentially affected by a merchant's data breach are less likely to use that financial institutions' payment cards in the future. Decreased payment card use decreases the financial institutions' revenue and, moreover, frequently leads to a decrease in the financial institution's reputation.

114. As such, in the wake of a data breach, financial institutions assess the most appropriate responsive action to both prevent fraudulent transactions and to ensure customers have their payment cards available for use. Financial institutions may also receive communications from their customers who are potentially affected by a data breach or who have questions about the breach. In many instances, financial institutions determine that the most effective response to a data breach is to reissue some or all of their alerted-on cards.

115. Once a financial institution becomes aware that it has potentially compromised payment cards, it faces a long-term risk of harm. The U.S. Government Accountability Office's research into the effects of data breaches found that "in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been

sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot rule out the significant risk of future harm."

116. Sonic had every opportunity to take preventive measures to avoid a breach of its POS systems. First, Sonic had more than adequate notice about the potential for hackers to infiltrate POS systems and rob customers of their credit and debit card information. Second, Sonic appreciated the consequences of such a breach, having witnessed Wendy's, Arby's and other major competitors experience data breaches in 2016 and 2017, and other merchants such as Target and Home Depot experience breaches between 2013 and 2014. Third, Sonic had access to information from data security experts, the FTC, and the Payment Card Industry identifying steps necessary to protect POS systems. Fourth, Sonic had available established guidelines from PCI DSS that offered at least, minimal levels of protection. Fifth, Sonic had recently replaced its POS systems and created a Brand Technology Fund to advance technology and cybersecurity enhancements. Despite the resources indicating the risk of a POS data breach and the potential steps to prevent such a breach, Sonic failed to take reasonable and sufficient action to avoid a breach of its POS systems, including failing to meet even minimal data security requirements like PCI DSS. While Sonic saved money by deliberately truncating its data security investments, it knowingly put itself at risk of a breach and Plaintiffs and Class at risk of incurring expenses necessary to remediate and limit the damages caused by a breach.

117. Had Sonic remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Sonic may have prevented the Data Breach involving its POS systems and ultimately, the theft of millions of customers' purchasing information.

118. Because Sonic failed to take reasonable protective measures to prevent the Data Breach, Plaintiffs and the Class have been and will continue to be required to bear the costs of preventing and repaying fraudulent transactions made with credit and debit card information obtained through Sonic's POS systems.

119. As a direct and proximate result of Sonic's Data Breach, Plaintiffs and the Class have suffered damages and injuries, including expenses related to the following: (a) cancelling or reissuing credit and debit cards affected by Sonic's Data Breach; (b) closing any deposit, transaction, checking, or other accounts affected by Sonic's data breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) opening or reopening any deposit, transaction, checking, or other accounts affected by Sonic's Data Breach; (d) refunding or crediting cardholders to cover the cost of any unauthorized transactions relating to Sonic's Data Breach; (e) responding to a higher volume of cardholder complaints, confusion, and concern; (f) increasing fraud monitoring efforts; (g) analyzing the risk to open accounts; and, (g) investigating the impact of the breach on the financial institution and its members.

120. In this case, Sonic's Data Breach compromised an estimated 5 million payment cards. The Credit Union National Association estimates the average cost to reissue payment cards is $8.02 per card[57], meaning financial institutions may have spent as much as $40.1 million in card reissuance costs alone as a result of the Data Breach. The cost may be even greater for EMV cards, which are more expensive to replace.

121. Additionally, because the payment card information stolen from Sonic and offered on Joker's Stash pre-dated discovery of the Data Breach, the risk of fraudulent charges is increased

[57] *Visa tiers reimbursement costs for reissuing breached cards*, Credit Union Nat'l Assoc. (May 21, 2015), https://news.cuna.org/articles/106029-visa-tiers-reimbursement-costs-for-reissuing-breached-cards.

because financial institutions, like Plaintiffs and the Class, did not have the opportunity to preemptively cancel and reissue cards upon receipt of an alert from the Card Brands of potentially fraudulent activity or of a potentially compromised card. Without advanced notice to financial institutions, purchasers of the stolen payment card information had a prolonged period to use or replicate the payment cards and make fraudulent purchases.

122. As a result of Sonic's Data Breach, Plaintiffs and the Class likely incurred tens of millions of dollars in actual damages related to remediating and mitigating the consequences of the Data Breach, including the fraudulent use of payment card data.

CLASS ALLEGATIONS

123. Plaintiffs bring this action on behalf of themselves and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that received an alert of one or more compromised accounts due to the Sonic Data Breach.

124. Excluded from the class is Sonic and its subsidiaries and affiliates; all employees of Sonic; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

125. Plaintiffs reserve the right to, after conducting discovery, modify, expand or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

126. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiffs believe that there are thousands of members of the Class. The number of alerts notifying

financial institutions of compromised card payment information per se indicates that the Class is numerous; however, 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.

127. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Sonic knew or should have known of the susceptibility of its POS systems to the Data Breach;

b. Whether Sonic controlled and took responsibility for protecting franchisee POS systems;

c. Whether Sonic's security measures were reasonable in light of the PCI DSS requirements, FTC data security recommendations, state laws and guidelines, and common recommendations made by data security experts;

d. Whether Sonic owed Plaintiffs and the Class a duty to implement reasonable security measures;

e. Whether Sonic's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to a breach of its duty to institute reasonable security measures;

f. Whether Sonic's failure to implement reasonable data security measures allowed the breach of its POS data systems to occur;

g. Whether Sonic's requirements that franchisees use insecure configurations caused the Data Breach;

h. Whether reasonable security measures known and recommended by the data security community could have prevented the breach of Sonic's POS systems;

i. Whether Plaintiffs and the Class were injured and suffered damages or other losses because of Sonic's failure to reasonably protect its POS data systems and corporate network; and

j. Whether Plaintiffs and the Class are entitled to relief.

128. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs are typical members of the Class. Each Plaintiff is a credit union that issued payment cards compromised by the exfiltration and theft of card payment information during Sonic's Data Breach. Plaintiffs' injuries are similar to other class members and Plaintiffs seek relief consistent with the relief due to the Class.

129. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Sonic to obtain relief for themselves and for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs have also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

130. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the 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 a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as

compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

131. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CLAIMS

COUNT I
Negligence

132. Plaintiffs repeat and re-allege the allegations contained in every preceding paragraph as if fully set forth herein.

133. Sonic owed an independent duty to Plaintiffs and the members of the Class to take reasonable care in managing and protecting payment card data. This duty arises from multiple sources.

134. At common law, Sonic owed an independent duty to Plaintiffs and the Class to implement reasonable data security measures because it was foreseeable that Sonic's data systems and the payment card data those systems processed would be targeted by hackers and that, should a breach occur, Plaintiffs and the Class would be harmed. Sonic controlled franchisee technology, infrastructure, and cybersecurity, and curtailed franchisees' ability to select technologies that would enhance data security. Sonic knew or should have known that if hackers breached its data systems, they would extract payment card data and inflict injury upon Plaintiffs and the Class. Furthermore, Sonic knew or should have known that if hackers accessed payment card data, Plaintiffs and the Class would be responsible for remediating and mitigating the consequences of a breach by cancelling and reissuing payment cards to their members and reimbursing their members for fraud losses, thereby incurring costs and damages as a direct result of Sonic's Data

Breach. Therefore, the Data Breach, and the harm is caused Plaintiffs and the Class, was the foreseeable consequence of Sonic's unsecured, unreasonable data security measures.

135. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Sonic to take reasonable measures to protect cardholder data and is a source of Sonic's duty to Plaintiffs and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FCT, the unfair act or practice by retailers, restaurants and other businesses like Sonic of failing to use reasonable measures to protect card holder data. Sonic, therefore, was required and obligated to take reasonable measures to protect payment card data Sonic may possess, hold, or otherwise use. The FTC publications and data security breach orders described herein further form the basis of Sonic's duty to adequately protect sensitive card payment information. By failing to implement reasonable data security measures, Sonic acted in violation of § 5 of the FTCA. Moreover, state consumer protection statutes and deceptive and unfair trade practices statutes incorporate and prohibit the unfair conduct prohibited under § 5 of the FTCA.

136. Sonic is obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which Sonic is bound. Industry standards are another source of duty and obligations requiring Sonic to exercise reasonable care with respect to Plaintiffs and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class. These include PCI DSS, the bear minimum data security measures Sonic was obligated to meet.

137. Sonic breached its duty to Plaintiffs and the Class. Specifically, Sonic prohibited franchisees from adopting reasonable data security measures, and failed to require franchisees to implement adequate systems, procedures, and personnel necessary to prevent the theft of payment

card data of Plaintiffs and the Class's members or customers. Sonic's unreasonable actions include violating PCI DSS by requiring franchisees to permanently enable remote access; providing insecure credentials to third parties; using technologies that were no longer supported by security patches; failing to utilize EMV-capable POS systems; implementing ineffective security monitoring technologies and procedures; failing to implement point-to-point encryption; and other unreasonable data security measures that foreseeably caused the Data Breach and which Sonic knew or should have known were unreasonable.

138. Sonic was fully capable of preventing the Data Breach. Sonic knew of data security measures required or recommended by the PCI DSS, the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or, even if its POS systems were compromised, would have limited the scope and length of the breach. Sonic established a Brand Technology Fund specifically to fund technology initiatives, which should have, but did not, include data security projects. Sonic thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

139. As a direct and proximate result of Sonic's negligence, Plaintiffs and the Class have suffered and will continue to suffer injury, including, but not limited to cancelling and reissuing payment cards; changing or closing accounts; notifying customers that their cards were compromised; analyzing the risk to open accounts; investigating claims of fraudulent activity; refunding fraudulent charges; increasing fraud monitoring on potentially impacted accounts; and taking other steps to protect themselves and their members or customers. Plaintiffs and the Class also lost interest and transaction fees due to reduced card usage resulting from the Data Breach, and the cards they issued (and the corresponding account numbers) were rendered worthless by their exposure during the Data Breach.

COUNT II
Negligence *Per Se*

140. Plaintiffs repeat and re-allege the allegations contained in every preceding paragraph as if fully set forth herein.

141. Sonic's unreasonable data security measures and failure to timely Plaintiffs and the Class of the Data Breach violate Section 5 of the FTCA, the Oklahoma Breach Notification Act ("OBNA"), and the Oklahoma Consumer Protection Act ("OCPA"). Although neither the FTCA nor the OBNA create a private right of action, both require businesses to institute reasonable data security measures and breach notification requirements, which Sonic failed to do. Similarly, the OCPA prohibits businesses from acting unfair or deceptively.

142. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants and other businesses like Sonic of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described above also form the basis of Sonic's duty.[58]

143. Sonic violated Section 5 of the FTCA by failing to use reasonable measures to protect payment card data and by not complying with applicable industry standards, including PCI DSS. Sonic's conduct was particularly unreasonable given the nature and amount of payment card data it obtained and the foreseeable consequences of a Data Breach at a national restaurant, including the immense damages that would result to consumers and financial institutions like Plaintiffs and the Class.

144. Sonic's violation of Section 5 of the FTCA constitutes negligence per se.

[58] *See supra*, note 75 (listing orders).

145. Plaintiffs and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect because they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiffs and many class members are credit unions, which are organized as cooperatives whose members are consumers.

146. Additionally, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. The FTC has pursued over fifty 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 suffered by Plaintiffs and the Class.

147. The OBNA provides: "Federal and State Laws require that if you maintain . . . a consumer's name and other personal identification numbers" including "credit card or financial information," such information is required to be "encrypted or redacted so that in the event of a breach, such information cannot be obtained and used by a third party." Additionally, the OBNA states:

> An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

148. The OBNA requires any notice to be provided "without any reasonable delay."

149. The OBNA indicates a state-created policy that entities acting within Oklahoma not put Oklahoma residents at risk by implementing unreasonable data security measures, including failing to encrypt personal information stored on any entity's systems. Similarly, the OBNA

requires entities who experienced a breach to notify residents whose personal information was reasonably believed to have been accessed.

150. Plaintiffs and the Class are within the class of individuals intended to be protected by the OBNA. The OBNA includes payment card information in the definition of "Personal information." § 162(6). Additionally, by requiring notice upon discovery of a breach, the OBNA ensures Financial Institutions can prevent fraudulent transactions from occurring, thus protecting financial institutions from additional harm caused by the Data Breach.

151. Sonic breached the OBNA by failing to provide reasonable notice of the breach to affected consumers. By violating the OBNA, Sonic committed negligence per se.

152. The OCPA prohibits, among other things, businesses from "[c]omit[ting] an unfair or deceptive trade practice as defined in Section 752 of this title[.]" 15 OK Stat. § 15-753.

153. The OCPA defines an "unfair trade practice" as "any practice which offends established public policy or . . . is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." Id. at 15-752(14).

154. The OCPA further defines a "deceptive trade practice" as "a misrepresentation, omission or other practice that has deceived or could reasonably be expected to deceive or mislead a person to the detriment of that. Such a practice may occur before, during or after a consumer transaction is entered into . . . ." Id. at § 15-752 (13).

155. Sonic acted unfairly under the OCPA by deliberately neglecting to institute reasonable data security measures, foreseeably increasing the likelihood of a data breach and the ensuing harm to financial institutions. While Sonic saved money be choosing not to adequately invest in its data security measures, it increased the risk of harm to the financial institutions that would be responsible for remediating the damages of a breach, including replacing compromised

cards and reimbursing consumers for fraud on their accounts attributable to the payment card information stolen from Sonic during the Data Breach. Sonic knowingly, deliberately, and unfairly placed the onus of paying to rectify its insecure data security measures on plaintiffs.

156. Sonic also acted deceptively by failing to inform consumers and financial institutions that it had implemented unreasonable data security measures. Sonic's practice of accepting credit and debit card payments for its goods and services represents to the public and to the financial industry that it has implemented the necessary data security measures to keep payment card information safe. Despite representing that its systems were secure, Sonic used outdated and insecure data security measures that eventually allowed hackers to breach its systems for months without notice. Sonic's actions misled consumers and the financial industry as to the state of its data security.

157. Plaintiffs and the Class are within the class of individuals intended to be protected by the OCPA. The OCPA is intended to protect both businesses and individuals from unfair and deceptive conduct and to facilitate consumer transactions. Financial institutions, like Plaintiffs and the Class, are a necessary part of consumer transactions because they facilitate payment using checks, credit cards, debit cards, and other means.

158. As a direct and proximate result of Sonic's negligence per se, Plaintiffs and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, analyzing the risk to open accounts; investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. Plaintiffs and the Class also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards

they issued (and the corresponding account numbers) were rendered worthless by their exposure during the Data Breach.

159. Because no statutes of other states are implicated, Oklahoma common law applies to Plaintiffs and the Class's negligence per se claim.

COUNT III
Declaratory and Injunctive Relief

160. Plaintiffs repeat and re-allege the allegations contained in every preceding paragraph as if fully set forth herein.

161. 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 those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

162. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the payment card data of Plaintiffs and the Class. Plaintiffs allege Sonic's actions (and inaction) in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiffs and the Class issued.

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

a. Sonic owes a legal duty to secure the sensitive financial information with which it is entrusted, specifically including information pertaining to credit and debit cards used by

persons who make purchases at Sonic restaurants, and to notify financial institutions of a Data Breach under the common law, Section 5 of the FTCA, the OBNA, the OCPA, Card Operating Regulations, PCI DSS standards, and various state statutes;

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

c. Sonic's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

164. The Court should also issue corresponding injunctive relief requiring Sonic to employ adequate security protocols consistent with industry standards to protect its customers' payment card data.

165. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Sonic's data systems. If another breach of Sonic's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they 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 their 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.

166. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Sonic if an injunction is issued. Among other things, if Sonic suffers another data breach, Plaintiffs and the Class will likely incur millions of dollars in damage. On the other hand, the cost to Sonic of complying with an injunction by employing reasonable data security measures

is relatively minimal, particularly given Sonic's pre-existing legal obligation to employ such measures.

167. 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, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

168. Wherefore, Plaintiffs, on behalf of themselves and the Class, request that this Court award relief against Sonic as follows:

a. An order certifying the class and designating Plaintiffs as the Class Representatives and their counsel as Class Counsel;

b. An Award to Plaintiffs and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiffs and the Class;

d. Injunctive relief to Plaintiffs and the Class;

e. An Award of attorneys' fees and costs as allowed by law; and

f. An Award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

169. Plaintiffs hereby demand a jury trial for all of the claims so triable.

Dated: October 21, 2019

/s/ Brian C. Gudmundson

Brian C. Gudmundson
Michael J. Laird
James W. Anderson
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
michael.laird@zimmreed.com
james.anderson@zimmreed.com

Charles H. Van Horn
Katherine M. Silverman
Lauren S. Frisch
BERMAN FINK VAN HORN P.C.
3475 Piedmont Road, NE, Suite 1100
Atlanta, GA 30305
Telephone: (404) 261-7711
Facsimile: (404) 233-1943
cvanhorn@bfvlaw.com
ksilverman@bfvlaw.com
lfrisch@bfvlaw.com

Interim Co-Lead Counsel for Plaintiffs and the Class

Joseph P. Guglielmo
Erin Green Comite
Margaret Ferron
SCOTT+SCOTT ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
ecomite@scott-scott.com
mferron@scott-scott.com

Karen Sharp Halbert
William R. Olson
ROBERTS LAW FIRM P.A.
20 Rahling Circle
Little Rock, AR 72223
Telephone: (501) 821-5575
Facsimile: (501) 821-4474
karenhalbert@robertslawfirm.us
williamolson@robertslawfirm.us

Arthur M. Murray
Stephen B. Murray, Sr.
Caroline Thomas 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
smurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Executive Committee for Plaintiffs and the Class

CERTIFICIATE OF SERVICE

This is to certify that I have this day served a true and correct copy of the foregoing ***Amended Class Action Complaint*** with the Clerk, United States District Court, using the CM/ECF system, which will automatically send e-mail notification to counsel of record, and sent a courtesy copy of the same via electronic mail to the following attorneys of record:

Kari M. Rollins	krollins@sheppardmullin.com
David Poell	dpoell@sheppardmullin.com
Craig C. Cardon	ccardon@sheppardmullin.com

Dated: October 21, 2019

/s/ Brian C. Gudmundson

Brian C. Gudmundson
Michael J. Laird
James W. Anderson
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
michael.laird@zimmreed.com
james.anderson@zimmreed.com