IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FORT MCCLELLAN CREDIT UNION, on behalf of itself and all others similarly situated, Plaintiff, v. ARBY'S RESTAURANT GROUP, INC., Defendant.	Case No. Hon. **CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT

Plaintiff Fort McClellan Credit Union ("Plaintiff" or "Fort McClellan CU") by its undersigned counsel, brings this action on behalf of itself and on behalf of a class of all similarly situated financial institutions and other entities against Arby's Restaurant Group, Inc. ("Defendant" or "ARG"). Plaintiff alleges upon personal knowledge those facts as to itself and its own acts, and upon information and belief as to all other matters, and states the following:

INTRODUCTION

1. This action arises out of a data breach at Arby's restaurants throughout the United States owned and operated by ARG. Massive data breaches have occurred to several businesses in the United States, including Target, Home Depot, and Wendy's restaurants, via malicious software installed remotely on businesses' point-of-sale ("POS") systems. These systems are used for managing customer payment transactions, including payments made with debit and credit cards.

2. The susceptibility of POS systems to malware is well-known. POS systems have been targeted by hackers looking to steal customer purchasing information since 2005. In the last five years, malware placed on POS systems has caused massive data breaches compromising millions of credit cards. Data security experts have warned, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[1]

3. Despite the susceptibility of POS systems, measures can be taken to prevent intrusion into POS devices and networks and to limit the effect of an intrusion if it occurs. For example, one data security expert recommends the "Tripod

[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#.

of POS Security," including: (1) utilizing POS systems supporting 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 meaningless series of letters and numbers, rendering any information collected by hackers meaningless.[2]

4. Additionally, the FTC has issued guidance and resources for businesses to advance their data security and the payment card industry has issued standards mandating merchants to meet certain minimum data security requirements.

5. ARG fully knew of the consequences of a data breach, the susceptibility of POS systems, and available measures to enhance data security. Yet, in or around October 2016, computer hackers infiltrated ARG's POS data systems via malicious software at its corporate-owned Arby's restaurants.[3]

6. From October 2016 to January 2017, the malware on ARG's POS systems went completely unnoticed by ARG. ARG did not became aware its systems were compromised until January 2017, when notified by the PSCU, a Credit

[2] *Id.*

[3] Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KrebsOnSecurity (Feb. 17, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/.

Union Service Organization. Although ARG knew of the breach in January, it made no public announcement about the breach and provided no information to financial institutions that issued compromised payment cards. In fact, the breach became public only after Brian Krebs, a data security investigator, reported on his blog, KrebsOnSecurity, that ARG had suffered a data breach via malware placed on Arby's restaurant's POS systems.[4] Since then, ARG admitted in an announcement that its systems had been breached compromising customer card payment information.[5]

7. Although Arby's has declined to disclose how long the malware was on its systems, a notice from PSCU stated that the breach is estimated to have lasted between Oct. 25, 2016 and January 19, 2017. Therefore, for nearly three months, hackers stole Arby's customers' debit and credit card information, including card numbers, completely unnoticed by ARG.

8. ARG's data breach at its Arby's restaurants was the inevitable result of ARG's inadequate data security measures. Despite the well-publicized and ever-growing threat of data breaches involving payment card networks and systems, ARG

[4] *Id.*

[5] *Security*, Arbys.com (last visited, Feb. 28, 2017), http://arbys.com/security/.

failed to ensure that it maintained adequate data security measures that could have detected and prevented the data breach.

9. In addition to failing to detect or prevent the intrusion and failing to implement data security measures that would have limited the effect of a breach on cardholders and the financial institutions who issued the cards, Defendant exacerbated injury by failing to notify customers of the infiltration when it supposedly learned of the breach in January.

10. Had Arby's implemented reasonable data security processes and procedures—measures known and recommended by the payment card industry, the Federal Trade Commission, and data security experts—ARG could have reasonably prevented the breach of its systems, or minimized the impact.

11. ARG's data breach caused substantial injury to financial institutions who issued cards affected by the data breach, including, but not limited to, costs to: (a) cancel or reissue any credit and debit cards affected by ARG's data breach; (b) close deposit, transaction, checking, or other accounts affected by ARG's data breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) open or reopen any deposit, transaction, checking, or other accounts affected by ARG's data breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to ARG's data breach; (e)

respond to a higher volume of cardholder complaints, confusion, and concern; and (f) increase fraud monitoring efforts.

12. In addition, ARG's data breach caused Plaintiff and the Class to lose revenue as a result of decreased card usage after the breach was disclosed to the public.

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

14. This class action is brought on behalf of financial institutions throughout the country to recover the costs that they and others similarly situated have been forced to bear as a direct result of the data breach of ARG's systems and to obtain other equitable relief. Plaintiff asserts claims for negligence and declaratory and injunctive relief.

JURISDICTION AND VENUE

15. 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 from ARG. Plaintiff, being organized in Alabama and operating its principal place of business in Alabama, is diverse from Defendant, operating its principal place of business in Georgia and being incorporated in Delaware. There are more than 100 putative class members.

16. This Court has personal jurisdiction over ARG because Defendant maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. ARG intentionally availed itself of this jurisdiction by accepting and processing payments for its foods and other services within Georgia.

17. Venue is proper under 18 U.S.C. §1391(a) because ARG's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

18. Plaintiff Fort McClellan CU is a nonprofit financial cooperative charted in 1953 that operates exclusively in northern Alabama. Plaintiff has five branches

in Alabama located in Anniston, Roanoke, Jacksonville, Ohatchee, and Centre. Plaintiff issues VISA payment cards and received alerts that some cards issued by Plaintiff may have been compromised by ARG's data breach. As a result of ARG's failure to adequately protect its data systems, Plaintiff has suffered, and continues to suffer, injury, including but not limited to: costs to cancel and reissue cards compromised in the data breach, costs to investigate and refund fraudulent charges; and administrative and operational costs in responding to the data breach on behalf of itself and its members.

19. Defendant Arby's Restaurant Group, Inc. is incorporated in Delaware and operates its principal place of business at 1155 Perimeter Center West, Atlanta, Georgia. Globally, there are more than 3,300 corporate-owned and franchised Arby's restaurants in operation. ARG owns and operates more than 1,000 of these restaurants. Arby's restaurants owned and operated by ARG accept payment for its goods and services through its POS network. Consumers' payment cards, which are issued by Plaintiff and the Class, are swiped at POS terminals located in Arby's restaurants to pay for goods and services received at Arby's restaurants.

STATEMENT OF FACTS

A. Background on Data Breaches Involving Malware on Company Point-of-Sale Systems.

20. A wave of data breaches causing the intrusion into and theft of consumer financial information has hit the United States.[6] In 2016, the number of U.S. data breaches surpassed 1,000, a record high. 2016 saw a forty percent increase in the number of data breaches as compared to 2015, which saw 780 reported data braches.[7] The number of compromised debit and credit cards in such a breach can be massive. For example, in 2013 and 2014 alone, the number of compromised cards was estimated to be over 100 million.[8]

21. Many of the massive data breaches occurring with the last four years involved malware placed on company point-of-sale ("POS") systems. For example, in 2013, hackers infiltrated Target, Inc.'s POS system stealing information from an estimated 40 million payment cards in the United States.[9] In 2014, over 7,500 self-checkout POS terminals at Home Depot stores throughout the United States were affected by malware allowing hackers to obtain information for 56 million debit and

---

[6] *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.

[7] *Id.*

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

[9] Brian Krebs, *The Target Breach, By the Numbers*, KrebsOnSecurity (May 14, 2014), https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

credit cards.[10] In 2016, more than 1,000 Wendy's restaurant locations were infiltrated with malware that stole customer data via on-site POS systems for several months.[11]

22. A POS system is an on-site device which manages transactions from consumer purchases, both by cash and card. An individual paying for goods and services via debit or credit cards swipe the cards at the POS terminal. When an individual pays by swiping a credit or debit card at a POS system, "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."[12]

23. Before transmitting consumer purchasing information over the network, the POS system stores data from the card's magnetic stripe in plain text within the POS system's memory.[13] Debit and credit card information stored in the

[10] Brett Hawkins, *Case Study: The Home Depot Data Breach* 7 (SANS Institute, Jan. 2015), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367.

[11] 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.

[12] 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.

[13] *Id.* at 5.

POS system's memory even for a split moment is susceptible to being stolen via malware installed directly on the POS system. Although theft of consumer purchasing information via POS systems has been utilized by hackers since 2005, malware installed on POS systems has now become "one of the biggest sources of stolen payment cards"[14] and is the cause of recent massive data breaches at various retail stores and restaurants.

24. Despite the vulnerabilities of POS systems, available security measures and businesses practices can significantly reduce the likelihood that hackers successfully infiltrate business' POS systems and limit the effect of any malicious software installed on a POS device. The payment card industry (e.g., MasterCard, VISA, Discover, and American Express), data security organizations, state governments, and federal agencies have all implemented various standards and guidance on security measures designed to stymie intrusions into POS systems.

25. Adhering to guidance and standards suggested by data security organizations and federal agencies and following standards mandated by the payment card industry can significantly reduce the likelihood of a data breach. In fact, one report indicated over 90% of the data breaches occurring in 2014 were

[14] *Id.* at 3.

preventable. Instead, susceptibility to a data breach occurs when businesses fail to take adequate and available security measures, leaving their "point-of-sale system . . . fraught with vulnerabilities" and lacking "effective internal data security procedures."[15]

26. In this case, despite Defendant's awareness of the risk of data theft via malware installed on its POS systems and the widely available resources to prevent intrusion into its POS data systems, Defendant failed to take reasonable and sufficient protective measures. Defendant's POS systems were infiltrated in October 2016 by installation of malicious software which stole consumer debit and credit card information for several months before being brought to Defendant's attention by people and institutions outside the company.

B. Arby's Restaurant Group, Inc. Point-of-Sale System Breach and the Theft of Consumer Purchasing Information.

27. ARG operates a chain of fast-food restaurants specializing in roast beef and other protein-based sandwiches. The first Arby's restaurant opened in 1964 in Boardman, Ohio and since then, Arby's has expanded to nearly 3,300 stores

[15] Steven Trader, *Wendy's hit With Shareholder Suit Over Customer Data Breach*, Law360 (Dec. 16, 2016), https://www.law360.com/articles/873987/wendy-s-hit-with-shareholder-suit-over-customer-data-breach.

globally, including 1,000 restaurants owned and operated by ARG and several thousand stores operating under a franchisee license.

28. Arby's restaurants have proved to be profitable, raking in annual sales of approximately $1.12 billion in 2015.[16] In the first quarter of 2016, Arby's posted 5.8% U.S. same-store sales growth, the twenty-second consecutive quarter Arby's has seen growth in that sector and the thirteenth straight quarter of outperforming the industry as a whole.[17]

29. With its growing profitability, Arby's has heavily invested in remodeling its restaurants. In 2014, Arby's launched its "Inspire Design" restaurant, a remodeling effort which Arby's claims has boosted sales by 15% at remodeled restaurants.[18] In 2015, nearly 200 of Arby's 3,300 locations were remodeled and upgraded to fit their new brand with plans to continue to remodel restaurants in 2016 and beyond.[19]

---

[16] Beth Kowitt, *How Arby's (Yes, Arby's) Is Crushing It*, Fortune (Apr. 27, 2016), http://fortune.com/2016/04/27/arbys-sales-growth/.

[17] *Id.*

[18] *Brand Milestones*, Arbys.com (last visited, Feb. 28, 2018), http://arbysfranchising.com/research/brand-milestones/.

[19] Beth Kowitt, *How Arby's (Yes, Arby's) Is Crushing It*, Fortune (Apr. 27, 2016), http://fortune.com/2016/04/27/arbys-sales-growth/.

30. Despite ARG's substantial investments made to modernize its branding and upgrade the appearance of its restaurants, ARG failed to make substantial and meaningful improvements to the security of its POS systems and administrative network placing the purchasing information of hundreds of thousands of its customers at risk.

31. ARG is, and at all relevant times was, fully aware of the consequences of a data breach of its POS systems. Just last year, Wendy's Restaurants' POS systems were compromised by malware which stole consumer purchasing information for over a half-year period. Wendy's shareholders claimed the "point-of-sale system . . . was fraught with vulnerabilities" and the company failed "to implement or enforce any effective internal data security procedures."[20]

32. Between 2008 and 2011, ARG and Wendy's International were merged into Wendy's/Arby's Group, Inc. Upon information and belief, Wendy's and Arby's used similar POS systems. Wendy's data breach put ARG on notice of the susceptibility of its system and the consequences of a data breach. Despite its

[20] Steven Trader, *Wendy's hit With Shareholder Suit Over Customer Data Breach*, Law360 (Dec. 16, 2016), https://www.law360.com/articles/873987/wendy-s-hit-with-shareholder-suit-over-customer-data-breach.

awareness of the dangers of a data breach, ARG failed to adequately and reasonably protect the payment card data of its customers.

33. ARG is, and at all relevant times was, fully aware of the significant volume of daily credit and debit card transactions at Arby's restaurants, amounting to tens of thousands of daily credit card transactions, and thus, the significant number of individuals who would be harmed by a breach of ARG's POS systems.

34. ARG is, and at all relevant times was, aware payment card data it maintains via credit and debit card transactions is highly sensitive and sought after, and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. ARG knew of the necessity of safeguarding its customers' Payment Card Data and of the foreseeable consequence that would occur if its data security systems were breached, including the significant costs that would be imposed on issuers, such as the Plaintiff, members of the Class, and others.

35. Despite its knowledge of the consequences of a data breach, ARG failed to take the necessary precautions to prevent intrusion into its own POS system. The first indication of a massive data breach occurred when PSCU, a Credit Union Service Organization that serves over 800 million credit unions, issued a non-public

alert advising credit unions that it had received a list of over 355,000 compromised credit card numbers from VISA and MasterCard.

36. Financial institutions have experienced an unprecedented number of alerts on member accounts—Compromised Account Management System ("CAMS") alerts for VISA members and Account Data Compromise Alters ("ADC alerts") for MasterCard members. CAMS and ADAC alerts are issued by VISA and MasterCard when some event jeopardizes the security of the financial institutions' customer accounts, *i.e.* card holders.

37. The massive number of alerts indicating credit and debit card information had been compromised is "generally a sign of a sizeable nationwide breach." In fact, the number of CAMS and ADC alerts received by many financial institutions were among the largest number of alerts received for a single event, indicating a significant number of compromised credit and debit cards.

38. The alert also indicated that Track 1 and Track 2 data may have been compromised by the breach, meaning cardholder names, primary account numbers, expiration dates, and in some cases, PIN numbers were all compromised. The length of exposure, or the "exposure window," was at least a three month period between October 25, 2016 to January 19, 2017. Thus, for at least three months intruders were able to collect Arby's customers' credit and debit card information unnoticed.

39. Eventually, the cause of the numerous compromised debit and credit cards was discovered when numerous financial institutions traced the alerts issued for their customers' accounts. Financial institutions identified the common transaction: purchases at an Arby's restaurant.

40. The breach became public on February 9, 2017 through an article published by Brian Krebs of KrebsOnSecruity, a leading information security investigator. KrebsOnSecurity announced that it reached out to ARG after hearing from several financial institutions about a suspected data breach at Arby's restaurants. In response to Kreb's inquiry, an ARG representative confirmed that Arby's recently remediated a breach involving malicious software installed on payment card systems at hundreds of its restaurant locations nationwide.

41. According to Krebs, a spokesperson for ARG said that Defendant was first notified by industry partners in mid-January about a breach at some of its locations. ARG indicated that the breach involved malware placed on payment systems inside Arby's corporate stores. Over 1,000 corporate-owned Arby's restaurants exist nationwide, although Arby's claims that not all of these restaurants were impacted by the Arby's Data Breach.

42. Eventually, Arby's made an official public announcement admitting its systems had been breached. The announcement came approximately four months

after the breach began and one month after it was resolved. ARG, however, failed to provide any additional about the scope and extent of the breach. The announcement in full was:

> Arby's Restaurant Group, Inc. (ARG) was recently provided with information that prompted it to launch an investigation of its payment card systems. ARG immediately notified law enforcement and enlisted the expertise of leading security experts, including Mandiant. While the investigation is ongoing, ARG quickly took measures to contain this incident and eradicate the malware from systems at restaurants that were impacted. ARG reminds guests that it is always advisable to closely monitor their payment card account statements for any unauthorized activity. If guests discover any unauthorized charges, they should report them immediately to the bank that issued their card.

43. In its announcement, ARG failed to take responsibility for the breach of its POS system. Instead, it put the onus on consumers to identify and resolve any potential nefarious action caused by its failure to protect its customers' purchasing information: "ARG reminds guests that it is always advisable to closely monitor their payment card account statements for any unauthorized activity. If guests discover any unauthorized charges, they should report them immediately to the bank that issued their card."

44. ARG did not indicate, and still has not indicated, how long the malware was on its data systems or how long hackers were able to steal Arby's customers' payment card information.

45. ARG has also not definitively listed which restaurant locations were affected by malware placed on its POS. By comparison, when Wendy's POS systems were breached, they provided a website for customers to determine whether they had visited an affected location.[21]

46. Although ARG's announcement does not indicate the number of affected individuals or compromised debit and credit card information, PSCU indicated that more than 355,000 credit and debit cards issued by PCSU member banks were compromised.

47. Like the previous massive data breaches, ARG's data breach was the result of malware on its POS networks, allowing hackers to steal Arby's customers' payment card data inside the store from remote locations.[22]

48. ARG should have been on high alert to the susceptibility of its POS systems to data breaches. In 2015, security experts warned about the susceptibility of POS systems in restaurants.[23] One expert warned "[y]ou [c]an't [n]eglect POS

[21] *Payment Card Check*, Wendys.com (last visited, Feb. 28, 2017), https://payment.wendys.com/paymentcardcheck.html.

[22] *See* Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KrebsOnSecurity (Feb. 17, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/.

[23] Leebro POS, *5 Lessons To Learn From A Restaurant POS Security Breach*, Pointofsale.com (last visited, Feb. 28, 2017),

[s]ystem [s]ecurity" 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."[24] 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."[25]

49. Datacap Systems, Inc. wrote in early 2016, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business." The same article notes Verizon reported "99 percent of the time, POS environments were hacked in only a few hours… [and] in 98 percent of cases, hackers exfiltrated (a term of art in the data security industry) 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."[26]

50. A data breach is not, however, an inevitability of doing business. Significant measures and business practices can reduce the likelihood hackers can

---

https://pointofsale.com/201506256716/Restaurant/Hospitality/5-Lessons-to-Learn-from-a-Restaurant-POS-Security-Breach.html.

[24] *Id.*

[25] *Id.*

[26] *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#.

successfully intrude business' POS systems and limit the effect of any malicious software installed on the POS device. In fact, the Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, in its 2015 annual report, revealed that 90% of data breaches in 2014 were preventable. [27]Similarly, in 2014, Online Trust Alliance found that 740 million records were stolen in 2013 and that 89% of data breaches occurring in that year were avoidable.[28]

51. More than two years ago, a Symantec report listed vulnerabilities in POS systems that should be resolved to prevent entry into POS system and theft of consumer purchasing information.[29] First, Symanetc recommended "point to point encryption" implemented through secure card readers which encrypt credit card information in the POS system, preventing "RAM-scraping" malware which extracts card information through the POS memory while it processes the

---

[27] 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.

[28] Online Trust Alliance *2014 Data Protection & Breach Readiness Guide* (2014), https://otalliance.org/system/files/files/resource/documents/2014otadatabreachguide4.pdf.

[29] *See* Symantec, *A Special Report On Attacks On Point-of-Sale Systems* 6-8 (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf.

transaction. Second, Symantec highlighted the need to utilize updated software to avoid susceptibility in older operating systems being phased out, like Windows XP or Windows XP Embedded. Third, Symantec emphasized the need to implement EMV chips, which do not directly transmit credit card information.

52. Last year, Datacap Systems recommended similar preventative measures in what they called the "Tripod of POS Security." The "tripod" included (1) implementing POS systems supporting EMV chip-based payment cards; (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 random series of letters and numbers, rendering any information collected by hackers meaningless.[30]

53. The payment card industry (MasterCard, VISA, Discover, JCB, and American Express) has also heightened security measures in their Card (or sometimes, Merchant) Operating Regulations. They require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even

[30] *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#.

in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

54. The payment card industry, like Symantec and DataSystems, has also strongly encouraged the use of POS terminals capable of accepting payment from EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used 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 hackers making it much more difficult for criminals to profit from what is stolen.

55. The Payment Card Industry ("PCI") Council emphasized that: "Card brands expect merchants' POS terminals and software to be EMV-capable by October 1, 2015."[31] Additionally, Card Operating Regulations shifted liability for

[31] PCI Security Standards Council, *Merchant Guide: Stepping Up to EMV Chip With PCI* (2015), https://www.pcisecuritystandards.org/pdfs/Merchant_Guide_-_Stepping_Up_to_EMV_Chip_with_PCI_-v06.pdf.

card-present fraudulent transactions to those merchants who failed to install POS devices capable of receiving cards with EMV chips by October 1, 2015.[32]

56. The PCI Security Standards Council, founded by American Express, Discover, JCB, MasterCard, and VISA, promulgates data security standards (referred to as "PCI DSS") developed 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."

57. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, sets forth detailed and comprehensive requirements that must be followed to meet each of the following twelve "high-level" mandates:

[32] EMV Migration Forum, *Understanding the 2015 U.S. Fraud Liability Shifts* (May 2015), http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf.

PCI Data Security Standard – High Level Overview

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

58. Among other things, PCI DSS required Defendant to: properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

59. Compliance with PCI DSS is required, but comprises the minimum protective action a business must take. Even in 2014, security experts recognized, "[w]hile PCI-DSS provides a framework for improved payment processing, it is clear that it has been insufficient to ensure the security of modern retail POS systems.

To truly improve the security posture of POS devices, organizations must take a more dynamic approach."[33] In fact, "every company that has been spectacularly hacked in the last three years has been PCI compliant."[34] Target, Wendy's Home Depot, Neiman Marcus, Michael's stores, Sally Beauty Holdings, Inc., Supervalu, Albertson's and many other businesses subjected to data breaches were recognized as PCI DSS compliant at the time of the compromise.[35]

60. Federal and State governments have likewise sought to introduce security standards and recommendations to temper data breaches and resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. The FTC notes the need to factor security into all business decisionmaking.[36] Data security requires encrypting information stored on

[33] SANS, *Point of Sale Systems and Security: Executive Summary* 1 (Oct. 2014), https://www.sans.org/reading-room/whitepapers/analyst/point-sale-systems-security-executive-summary-35622.

[34] Sean M. Kerner, *Eddie Bauer Reveals It Was the Victim of a POS Breach*, eWeek (Aug. 19, 2016), http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach.html.

[35] SANS, *Point of Sale Systems and Security: Executive Summary* 1 (Oct. 2014), https://www.sans.org/reading-room/whitepapers/analyst/point-sale-systems-security-executive-summary-35622.

[36] Federal Trade Comm'n, *Start With Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015),

computer networks; holding on to information only as long as necessary; properly disposing of personal information that is no longer needed; limiting administrative access to business systems; using industry-tested and accepted security methods; monitoring activity on your network to uncover unapproved activity; verifying that privacy and security features work; testing for common vulnerabilities; and, updating and patching third-party software.[37]

61. The FTC has taken an active approach in issuing orders against businesses for failing to adequately and reasonably protect customer data. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as a unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

62. Several states have specifically enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code §1798.81.5(b) and Wash. Rev. Code

https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[37] *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.

§19.255, or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. §325E.64. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Most states have also enacted statutes requiring merchants to provide notice to consumers of security systems breaches. These statutes, explicitly or implicitly, mandate the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

63. In this case, ARG was at all times fully aware of its data protection obligations for all Arby's locations because of its participation in payment card processing networks. ARG was also aware of the significant repercussions of a data breach because of the numerous daily transactions of tens of thousands of sets of payment card data. Defendant further knew that because they accepted payment cards at Arby's locations that processed sensitive financial information, customers and financial institutions, including Plaintiff and the Class, were entitled to and relied upon ARG to keep sensitive information secure from hackers.

64. Despite ARG's understanding of the consequence of a data breach and the measures it could take to avoid a data breach, ARG, upon information and belief, failed to employ reasonable security measures to avoid, detect, and/or minimize the

impact of a POS data breach at its locations. This includes, but is not limited to, failure to comply with PCI DSS requirements; failure to take additional, reasonable protective measures beyond the PCI DSS; failure to implement EMV-capable POS systems by the October 1, 2015 deadline; operating POS systems with insufficient security in place; failure to enable point-to-point and end-to-end encryption and; failure to take reasonable and necessary protective measures on its administrative network.

65. The accumulation of ARG's failed security measures was the breach of its POS systems at its corporate-owned restaurants, numbering over 1,000 in the United States. ARG failed to even identify the intrusion for months, and not until card issuers and the payment card industry traced suspicious activity to Arby's restaurants.

66. ARG failed to reasonably protect cardholder information, putting consumer financial accounts in jeopardy and forcing financial institutions, like Plaintiff and the Class, to take remedial action to address ARG's inadequate security measures.

67. ARG had every opportunity to take preventive measures to avoid or minimize a breach of its POS systems. First, ARG 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, ARG was aware of the consequences of such a breach, having witnessed Wendy's, a major member of the same industry (and former sister company,) experience a breach in early 2016 and other large retailers like Target and Home-Depot experience breaches between 2013 and 2014. Third, ARG had access to information from data security experts, the FTC, and the payment card industry identifying steps necessary to protect POS systems. Fourth, ARG had available established guidelines from PCI DSS which offered at least, minimal levels of protection. Despite the resources indicating the degree of risk of POS intrusion and the potential steps to stymie a data breach, ARG failed to take reasonably and sufficient action to prevent a costly breach of its POS systems.

68. In addition to being aware and motivated to secure its POS data, ARG had every opportunity to do so. ARG recently implemented a plan to remodel and upgrade numerous Arby's restaurants throughout the United States with its "Inspire Design" image. Remodeling of its restaurants offered ARG an opportunity to update and enhance its in-store POS devices. However, upon information and belief, Arby's failed to do so. Additionally, since 2013, ARG has dramatically increased the profitability of Arby's restaurants and its overall annual gross profits. ARG made significant expenditures to market its products; modernize its restaurants; add

menu items; and, revitalize its brand. However, ARG failed to make significant investments in its data security, despite the growing number of POS intrusions.

69. Had ARG remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, ARG could have prevented intrusion into its POS system and ultimately, the theft many of its customers' purchasing information.

70. Because ARG failed to take reasonable protective measures to prevent a data breach, Plaintiff and the Class have been required to bear the costs of reissuing the affected cards and repaying fraudulent transactions made with credit and debit card information obtained through ARG's POS systems.

C. Fort McClellen Credit Union and Other Credit Unions Were Required to Remediate the Damage Caused by ARG's Data Breach.

71. As a result of ARG's data breach, Plaintiff and the Class were required to act immediately to mitigate the stolen card data and massive fraudulent transactions being made on payment cards that they had issued. Federal regulations ultimately protect consumers from most fraud loss, leaving Plaintiff and the Class to bear the brunt of data breaches, such as ARG's.

72. Fort McClellan CU is a credit union operating in five different locations in Alabama. Fort McClellan CU, like credit unions throughout the United States, received notice of cards potentially compromised by ARG's data breach. Fort

McClellan CU now must bear the costs of canceling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, monitoring potentially impacted accounts, and taking other measures to protect their operations and their members' financial accounts.

73. The ARG data breach resulted in the largest number of compromised credit and debit cards issued by Fort McClellan CU in the history of its operation.

74. Fort McClellan CU has suffered damage as a result of the ARG data breach, including but not limited to contacting affected members, refunding fraudulent transactions, and reissuing affected cards. This is in addition to the substantial disruption to Plaintiff's business operations as a result of the breach, requiring personnel to investigate, respond, and reach out to members regarding hundreds of alerted-on accounts.

75. The challenges and expenses Fort McClellan CU has already experienced and will continue to experience as it remediates the damages from ARG's breach are shared among the Class. Credit Unions and other card issuers throughout the country will be forced to shoulder the burden of ARG's data breach. Plaintiff and the Class have been forced to cancel and reissue payment cards, change or close accounts, notify members that their cards were compromised, investigate

claims of fraudulent activity, refund fraudulent charges, increase monitoring on potentially impacted accounts, and take other steps to protect themselves and their members. Furthermore, Plaintiff and the Class lose interest and transaction fees because of reduced card usage. The debit and credit cards belonging to Plaintiff and the Class and the account numbers on the face of the cards were devalued.

76. Plaintiff and the Class have suffered significant damages which will continue to increase to remedy the consequences of ARG's data breach.

CLASS ALLEGATIONS

77. Plaintiff brings this action on behalf of itself 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 seeks certification of the following Class:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from ARG while malware was installed on ARG's payment card systems.

78. Excluded from the Class are Defendant and its subsidiaries 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 and his/her immediate family and court staff.

79. Plaintiff reserves the right to 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 following discovery.

80. **Numerosity.** Consistent with Rule 23(a)(1), the Class is so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are thousands of members of the Class and the sheer number of alerts notifying financial institutions of compromised card payment information indicates the Class is numerous; however, the precise number of Class members is unknown to Plaintiff. 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.

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

a. Whether ARG knew or should have known of the susceptibility of their POS systems to a data breach;

b. Whether ARG's security measures to protect is POS systems were reasonable;

c. Whether ARG failed to comply with applicable security standards;

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

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

f. Whether reasonable measures to monitor and detect unauthorized activity known and recommended by the data security community could have minimized;

g. Whether Plaintiff and the Class were injured and suffered damages or other losses as a result of ARG's actions, or failures to act;

82. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff if a typical member of the Class. Plaintiff is a credit union who issued payment cards compromised by the infiltration and theft of card payment information from ARG's POS system. Plaintiff's injures are similar to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

83. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against ARG to obtain relief for it and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation in this type,

having previously litigated several data breach cases, including serving as lead counsel in the Target Data Breach litigation on behalf of financial institutions, and in leadership roles in the Home Depot, Wendy's, and Noodles & Co. data breach cases on behalf of financial institutions. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

84. **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, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small individually compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. 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.

85. **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.

COUNT I

Negligence

86. Plaintiff re-alleges the foregoing paragraph as if fully set forth herein.

87. ARG owed an independent duty to Plaintiff and the members of the class to take reasonable care in managing and protecting cardholder information, and to timely notify Plaintiff in the case of a data breach. This duty arises from multiple sources.

88. At common law, ARG owed an independent duty to Plaintiff and the Class because it was foreseeable that ARG's data systems and the cardholder data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract cardholder data from ARG's systems and misuse that information to the detriment of Plaintiff and the Class, and that Plaintiff and the Class would be forced to mitigate such fraud or such potential fraud by cancelling

and reissuing payment cards to their members and reimbursing their members for fraud losses.

89. ARG's common law duty also arises from the special relationship that existed between ARG and the Class. Plaintiff and the Class entrusted ARG with the cardholder data contained on the payment cards Plaintiff and the Class issued to their members. ARG, as the holder and processor of that information, was the only party who realistically could ensure that its data systems were sufficient to protect the data it was entrusted to hold.

90. In addition to the common law, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45, mandated Defendant to take reasonable measures to protect cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which requires and obligates ARG to take reasonable measures to protect any cardholder data ARG may hold or process. The FTC publications and data security breach orders described above further form the basis of ARG's duty to adequately protect sensitive card payment information. In addition, individual states have enacted statutes based upon the FTCA that also created a duty.

91. ARG is also obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which ARG is bound. The

industry standards create yet another source of obligations that mandate ARG to exercise reasonable care with respect to Plaintiff and the Class.

92. ARG, by its actions, has breached its duties to Plaintiff and the class. Specifically, Defendant failed to act reasonably in protecting the cardholder data of the members of Plaintiff and the Class, and did not have reasonably adequate systems, procedures and personnel in place to prevent the disclosure and theft of the cardholder data of Plaintiff and the Class' members.

93. ARG also had the opportunity and resources to prevent a data breach. ARG has increased significantly in profitability and has specifically emphasized remodeling its restaurants. ARG's remodeling efforts could have easily included updated POS systems and updated software to protect its customers' payment card information. ARG was fully aware of the possibility and consequence of a breach of its POS system. Additionally, the FTC, PCI, and other data security experts have proffered guidance and methods to enhance the security of POS data systems and networks. ARG, however, failed to take such action, leaving its data systems unreasonably vulnerable to a breach.

94. As a direct and proximate result of ARG's conduct, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying

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

95. Georgia law applies to the negligence claims of Plaintiff and the Class.

COUNT II

Negligence *Per Se*

96. Plaintiff re-alleges each of the preceding paragraphs as if fully set forth herein.

97. Section 5 of the Federal Trade Commission Act, 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 such as ARG of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described above also form the basis of ARG's duty.

98. ARG violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect cardholder data and by not complying

with applicable industry standards, including PCI DSS as described herein. ARG's conduct was particularly unreasonable given the nature and amount of cardholder data it obtained and stored and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to financial institutions like Plaintiff and the Class.

99. ARG's violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence *per se*.

100. Plaintiff 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, Plaintiff and many class members are credit unions, which are organized as cooperatives whose members are consumers.

101. 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 Plaintiff and the Class.

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

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

103. Georgia law applies to the negligence *per se* claims of Plaintiff and the Class.

COUNT III

Declaratory and Injunctive Relief

104. Plaintiff re-alleges each preceding paragraph as if fully set forth herein.

105. 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 here, that are tortious and which violate the terms of the federal and state statutes described herein.

106. 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 cardholder data of the members of Plaintiff and the Class. Plaintiff alleges ARG's actions (and inaction) in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff continues to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the Class members have issued.

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

a. ARG continues to owe a legal duty to secure the personal and financial information with which it is entrusted – specifically including information pertaining to credit and debit cards used by persons who made purchases at Arby's restaurants – and to immediately notify financial institutions of a data breach under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

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

c. ARG's ongoing breaches of its legal duty continue to cause Plaintiff harm.

108. The Court should also issue corresponding injunctive relief requiring ARG to employ adequate security protocols consistent with industry standards to protect the sensitive personal and financial information with which it is entrusted.

109. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of ARG's data systems. The risk of another such breach is real, immediate, and substantial. If another breach of ARG's data systems occurs, Plaintiff 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 Plaintiff for out of pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff, which include certain monetary damages that are not legally quantifiable or provable, and reputational damage.

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

relatively minimal and ARG has a pre-existing legal obligation to employ such measures.

111. 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 many consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

112. Wherefore, Plaintiff, on behalf of itself and on behalf of the other members of the proposed Class, requests that this Court order:

a. Certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;

b. Awarding Plaintiff and the proposed Class members damages with pre-judgment and post-judgment interest;

c. Entering a declaratory judgment in favor of Plaintiff and the Class as described herein;

d. Granting Plaintiff and the Class the injunctive relief requested herein;

e. Awarding attorneys' fees and costs as allowed by law; and

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

JURY TRIAL DEMANDED

113. Plaintiff hereby demands a jury trial for all of the claims so triable.

Dated: March 2, 2017

Respectfully submitted,

s/Pitts Carr
W. Pitts Carr
Georgia Bar No. 112100
Alex D. Weatherby
Georgia Bar No. 819975
CARR & WEATHERBY, LLP
10 North Parkway Square
4200 Northside Parkway, NW
Atlanta, Georgia 30327
(404) 442-9000
(404) 442-9700 Facsimile
www.wpcarr.com

Charles S. Zimmerman
Brian C. Gudmundson
Michael J. Laird
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400
charles.zimmerman@zimmreed.com
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com

Jonathan L. Kudulis
KUDULIS REISINGER PRICE
17 North 20th Street, Suite 350

Birmingham, AL 35203
Telephone: (205) 251-3151
jkudulis@trimmier.com

Attorneys for Plaintiff and the Proposed Class

JS44 (Rev. 11/16 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

FORT MCCLELLAN CREDIT UNION

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Calhoun County, MN
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

ARBY'S RESTAURANT GROUP, INC.

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton, GA
(IN U.S. PLAINTIFF CASES ONLY)

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

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Carr & Weatherby, 4200 N'side Pkwy NW, Bldg 10, Atlanta, GA 30327, 404-442-9000, pcarr@wpcarr.com, aweatherby@wpcarr.com; Zimmerman Reed, 1100 IDS Center, 80 S. 8th St. Minneapolis, MN, 55402, 612-341-0400, brian.gudmundson@zimmreed.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☐ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☐ 2	☐ 2	CITIZEN OF ANOTHER STATE	☑ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

- ☑ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Plaintiff alleges negligence, negligent per se, declaratory relief and injunction and Plaintiff brings these claims on behalf of a nationwide class of similarly situated entities.

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☑ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** over $5,000,000.00

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE_____ **DOCKET NO.**_____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)
- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

s/Pitts Carr 03/02/17

SIGNATURE OF ATTORNEY OF RECORD **DATE**